

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
)
Masahiro KOMURA, et al.)
) Group Art Unit: Unassigned
Serial No.: To be assigned)
) Examiner: Unassigned
Filed: December 20, 2000)



For: **A METHOD AND APPARATUS FOR MEDIATION OF SECURITY INFORMATION, AND A COMPUTER PRODUCT**

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

*Assistant Commissioner for Patents
Washington, D.C. 20231*

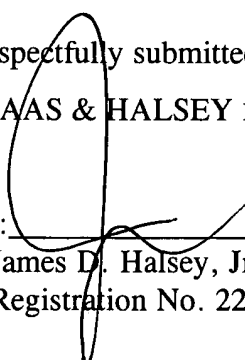
Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-234555
Filed: August 2, 2000.

It is respectfully requested that the applicants be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,
STAAS & HALSEY LLP

By: 
James D. Halsey, Jr.
Registration No. 22,729

Date: December 20, 2000
700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

JC853 U.S. PTO
09/739645
12/20/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 8月 2日

出 願 番 号

Application Number:

特願2000-234555

出 願 人

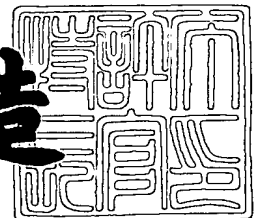
Applicant (s):

富士通株式会社

2000年10月27日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3089773

【書類名】 特許願

【整理番号】 0050561

【提出日】 平成12年 8月 2日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明の名称】 セキュリティ情報仲介装置、セキュリティ情報仲介方法
およびセキュリティ情報仲介プログラムを記録したコン
ピュータ読み取り可能な記録媒体

【請求項の数】 15

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内

【氏名】 小村 昌弘

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内

【氏名】 小谷 誠剛

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内

【氏名】 鳥居 悟

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100089118

【弁理士】

【氏名又は名称】 酒井 宏明

【手数料の表示】

【予納台帳番号】 036711

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9717671

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティ情報仲介装置、セキュリティ情報仲介方法およびセキュリティ情報仲介プログラムを記録したコンピュータ読み取り可能な記録媒体

【特許請求の範囲】

【請求項1】 情報提供者の情報提供者端末から提供されたセキュリティ情報を登録する登録手段と、

前記セキュリティ情報の有用性を判断する情報受信者の情報受信者端末へ、前記登録手段により登録された前記セキュリティ情報を転送する第1の転送手段と

当該セキュリティ情報の有用性を示す返答情報および当該セキュリティ情報の情報提供料の支払いに関する支払情報を前記情報受信者端末より受信する受信手段と、

前記返答情報および前記支払情報を前記情報提供者端末へ転送する第2の転送手段と、

を備えたことを特徴とするセキュリティ情報仲介装置。

【請求項2】 前記登録手段は、登録済みのセキュリティ情報を参照し、提供されたセキュリティ情報が新規である場合にのみ、当該セキュリティ情報を登録し、前記第1の転送手段は、提供されたセキュリティ情報が新規である場合にのみ、当該セキュリティ情報を前記情報受信者端末へ転送することを特徴とする請求項1に記載のセキュリティ情報仲介装置。

【請求項3】 前記情報受信者が所望するセキュリティ情報の分類情報を登録する分類情報登録手段と、前記情報提供端末から提供されたセキュリティ情報を分類する分類手段とを備え、前記第1の転送手段は、前記分類情報と前記分類手段の分類結果が一致する場合にのみ当該セキュリティ情報を前記情報受信者端末へ転送することを特徴とする請求項1または2に記載のセキュリティ情報仲介装置。

【請求項4】 前記受信手段は、当該セキュリティ情報の無効を示す無効情報を前記情報受信者端末より受信し、前記第2の転送手段は、前記無効情報を前

記情報提供者端末へ転送することを特徴とする請求項 1 ～ 3 のいずれか一つに記載のセキュリティ情報仲介装置。

【請求項 5】 前記受信手段は、有用性が示されたセキュリティ情報の対策用の修正情報を受信し、前記第 2 の転送手段は、前記修正情報を前記情報提供者端末へ転送することを特徴とする請求項 1 ～ 4 のいずれか一つに記載のセキュリティ情報仲介装置。

【請求項 6】 前記登録手段により登録された前記セキュリティ情報を公開する公開手段を備えたことを特徴とする請求項 1 ～ 5 のいずれか一つに記載のセキュリティ情報仲介装置。

【請求項 7】 前記登録手段により登録されたセキュリティ情報および前記修正情報を公開する公開手段を備えたことを特徴とする請求項 5 に記載のセキュリティ情報仲介装置。

【請求項 8】 情報提供者の情報提供者端末から提供されたセキュリティ情報を登録する登録工程と、

前記セキュリティ情報の有用性を判断する情報受信者の情報受信者端末へ、前記登録工程で登録された前記セキュリティ情報を転送する第 1 の転送工程と、

当該セキュリティ情報の有用性を示す返答情報および当該セキュリティ情報の情報提供料の支払いに関する支払情報を前記情報受信者端末より受信する受信工程と、

前記返答情報および前記支払情報を前記情報提供者端末へ転送する第 2 の転送工程と、

を含むことを特徴とするセキュリティ情報仲介方法。

【請求項 9】 前記登録工程では、登録済みのセキュリティ情報を参照し、提供されたセキュリティ情報が新規である場合にのみ、当該セキュリティ情報を登録し、前記第 1 の転送工程では、提供されたセキュリティ情報が新規である場合にのみ、当該セキュリティ情報を前記情報受信者端末へ転送することを特徴とする請求項 8 に記載のセキュリティ情報仲介方法。

【請求項 10】 前記情報受信者が所望するセキュリティ情報の分類情報を登録する分類情報登録工程と、前記情報提供端末から提供されたセキュリティ情

報を分類する分類工程とを含み、前記第 1 の転送工程では、前記分類情報と前記分類工程の分類結果が一致する場合にのみ当該セキュリティ情報を前記情報受信者端末へ転送することを特徴とする請求項 8 または 9 に記載のセキュリティ情報仲介方法。

【請求項 1 1】 前記受信工程では、当該セキュリティ情報の無効を示す無効情報を前記情報受信者端末より受信し、前記第 2 の転送工程では、前記無効情報を前記情報提供者端末へ転送することを特徴とする請求項 8 ～ 1 0 のいずれか一つに記載のセキュリティ情報仲介方法。

【請求項 1 2】 前記受信工程では、有用性が示されたセキュリティ情報の対策用の修正情報を受信し、前記第 2 の転送工程では、前記修正情報を前記情報提供者端末へ転送することを特徴とする請求項 8 ～ 1 1 のいずれか一つに記載のセキュリティ情報仲介方法。

【請求項 1 3】 前記登録工程で登録された前記セキュリティ情報を公開する公開工程を含むことを特徴とする請求項 8 ～ 1 2 のいずれか一つに記載のセキュリティ情報仲介方法。

【請求項 1 4】 前記登録工程で登録されたセキュリティ情報および前記修正情報を公開する公開工程を含むことを特徴とする請求項 1 2 に記載のセキュリティ情報仲介方法。

【請求項 1 5】 前記請求項 8 ～ 1 4 のいずれか一つに記載のセキュリティ情報仲介方法をコンピュータに実行させるためのセキュリティ情報仲介プログラムを記録したコンピュータ実行可能な記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、コンピュータプログラムの開発元（ベンダ）とユーザとの間で、セキュリティホールに関するセキュリティ情報を効率的に仲介させるセキュリティ情報仲介装置、セキュリティ情報仲介方法およびセキュリティ情報仲介プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

【 0 0 0 2 】

近時、コンピュータプログラムのセキュリティ情報に関する情報交換および情報公開は、CERTやその他のボランティア団体、民間企業により、インターネットを介して世界規模で行われている。ここでいうセキュリティ情報とは、コンピュータプログラムの設計上のミスやバグ等によってセキュリティ対策上問題となるセキュリティホールに関する情報をいう。

【0003】

しかしながら、現状では、セキュリティホールを発見した善意者が、危険なクラッカーと間違われたり、コンピュータプログラム開発会社とのトラブルに巻き込まれる等の問題が発生していることから、セキュリティ情報の交換および公開をオープンに誰もが行うことができる環境が整っているとは言い難い。これは、インターネットをはじめとするオープンシステムの流れに逆行し、人類共有の資産であるコンピュータプログラムの発展を阻害するものである。このような背景より、かかる問題を効果的に解決するための手段、方法が切望されている。

【0004】

【従来の技術】

コンピュータプログラムの開発元では、テスト段階で設計ミスやバグ等のセキュリティホールを徹底的に洗い出し、対策済みのコンピュータプログラムをユーザに提供している。しかしながら、現実的には、テスト段階でセキュリティホールの全てを発見することが極めて困難であるため、ユーザが当該コンピュータプログラムを利用してはじめて、開発元で発見できなかったセキュリティホールが発見される場合が多い。

【0005】

ここで、セキュリティホールを発見したユーザは、セキュリティホールの詳細情報をセキュリティ情報として、直接、開発元に提供したり、インターネット上のセキュリティ情報サイトにセキュリティ情報を投稿する等の対応を採る場合がある。この場合、開発元では、提供されたセキュリティ情報が有用であると判断すると、修正用のパッチプログラムや当該セキュリティ情報をユーザに提供する等の対応をとる。

【0006】

【発明が解決しようとする課題】

ところで、前述したように、従来では、直接やインターネット上のセキュリティ情報サイトを介して、ユーザから開発元へセキュリティ情報を提供する環境がある。しかしながら、従来では、善意でセキュリティ情報を提供したユーザが、危険なクラッカと酷評されたり、セキュリティホールの存在を公開したくない開発元とのトラブルに巻き込まれたりする場合が多い。

【0007】

従って、従来では、有用なセキュリティ情報を有するユーザが、上述した酷評やトラブルを避け、当該セキュリティ情報の提供を躊躇してしまう環境があることも否めない。このような環境は、コンピュータプログラムの質向上を妨げ、開発元およびユーザにとって利益とならない。

【0008】

一方、開発元では、インターネット上に分散されたセキュリティ情報を効率良く収集することが困難であり、しかも質にバラツキがあるセキュリティ情報の中から有用なものを選別しなければならないため、労力やコストも看過できない状況にある。ここで、分散されたセキュリティ情報を分類する動きがあるが、際だった成果が見られない。結局、開発元は、独自に大量のセキュリティ情報を収集し、この中から有用なものを選別するという従来の手法を踏襲せざるを得ないのである。

【0009】

本発明は、上記に鑑みてなされたもので、ユーザにとってセキュリティ情報を提供し易い環境を整備することができ、しかも開発元にとって低コストで有用なセキュリティ情報を収集することができるセキュリティ情報仲介装置、セキュリティ情報仲介方法およびセキュリティ情報仲介プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0010】

【課題を解決するための手段】

上記目的を達成するために、本発明は、情報提供者の情報提供者端末から提供されたセキュリティ情報を登録する登録手段と、前記セキュリティ情報の有用性

を判断する情報受信者の情報受信者端末へ、前記登録手段により登録された前記セキュリティ情報を転送する第1の転送手段と、当該セキュリティ情報の有用性を示す返答情報および当該セキュリティ情報の情報提供料の支払いに関する支払情報を前記情報受信者端末より受信する受信手段と、前記返答情報および前記支払情報を前記情報提供者端末へ転送する第2の転送手段とを備えたことを特徴とする。

【0011】

この発明によれば、情報提供者（ユーザ）よりセキュリティ情報が提供されると、登録手段によりセキュリティ情報が登録される。これにより、第1の転送手段により、上記セキュリティ情報が情報受信者端末（例えば、コンピュータプログラムの開発元の端末）へ転送され、情報受信者によりセキュリティ情報の有用性が判断される。ここで、セキュリティ情報が有用であると判断されると、情報受信者端末からは、返答情報および支払情報が送信される。

【0012】

そして、上記返答情報および支払情報が受信手段に受信されると、第2の転送手段は、返答情報および支払情報を情報提供者端末へ転送する。これにより、情報提供者は、自身が提供したセキュリティ情報が有用であることを認識するとともに、セキュリティ情報の提供に対する支払いがあることを認識する。

【0013】

このように、この発明によれば、情報提供者からのセキュリティ情報をダイレクトに情報受信者側に提供し、しかも有用なセキュリティ情報を提供した者に対して支払いを行うようにしたので、情報提供者（ユーザ）にとってセキュリティ情報を提供し易い環境を整備し、情報受信者（例えば、開発元）にとって低コストで有用なセキュリティ情報を収集することができる。

【0014】

また、本発明は、情報提供者の情報提供者端末から提供されたセキュリティ情報を登録する登録工程と、前記セキュリティ情報の有用性を判断する情報受信者の情報受信者端末へ、前記登録工程で登録された前記セキュリティ情報を転送する第1の転送工程と、当該セキュリティ情報の有用性を示す返答情報および当該

セキュリティ情報の情報提供料の支払いに関する支払情報を前記情報受信者端末より受信する受信工程と、前記返答情報および前記支払情報を前記情報提供者端末へ転送する第2の転送工程とを含むことを特徴とする。

【0015】

この発明によれば、情報提供者（ユーザ）よりセキュリティ情報が提供されると、登録工程でセキュリティ情報が登録される。これにより、第1の転送工程で上記セキュリティ情報が情報受信者端末（例えば、コンピュータプログラムの開発元の端末）へ転送され、情報受信者によりセキュリティ情報の有用性が判断される。ここで、セキュリティ情報が有用であると判断されると、情報受信者端末からは、返答情報および支払情報が送信される。

【0016】

そして、受信工程で上記返答情報および支払情報が受信されると、第2の転送工程では、返答情報および支払情報が情報提供者端末へ転送される。これにより、情報提供者は、自身が提供したセキュリティ情報が有用であることを認識するとともに、セキュリティ情報の提供に対する支払いがあることを認識する。

【0017】

このように、この発明によれば、情報提供者からのセキュリティ情報をダイレクトに情報受信者側に提供し、しかも有用なセキュリティ情報を提供した者に対して支払いを行うようにしたので、情報提供者（ユーザ）にとってセキュリティ情報を提供し易い環境を整備し、情報受信者（例えば、開発元）にとって低コストで有用なセキュリティ情報を収集することができる。

【0018】

【発明の実施の形態】

以下、図面を参照して本発明にかかるセキュリティ情報仲介装置、セキュリティ情報仲介方法およびセキュリティ情報仲介プログラムを記録したコンピュータ読み取り可能な記録媒体の実施の形態1～4について詳細に説明する。

【0019】

（実施の形態1）

図1は、本発明にかかる実施の形態1の構成を示すブロック図である。この図

において、ユーザクライアント 1 1 は、ユーザ 1 0 により操作されるコンピュータ端末であり、ネットワーク 1 2 を介してセキュリティ情報仲介装置 2 0 にアクセス可能とされている。ユーザ 1 0 は、後述する開発元 3 1 A や開発元 3 1 B、その他の開発元により開発された各種コンピュータプログラムを利用する者である。また、ユーザ 1 0 は、コンピュータプログラムのバグ等のセキュリティホールを発見し、これをセキュリティ情報として提供することができる知識を有する者である。

【 0 0 2 0 】

また、ユーザクライアント 1 1 は、ネットワーク 1 2 を介してセキュリティ情報仲介装置 2 0 にセキュリティ情報 4 0 を登録する機能と、セキュリティ情報 4 0 が有用である場合にセキュリティ情報仲介装置 2 0 から返答情報 4 1 A および支払情報 4 2 を受信する機能とを備えている。このセキュリティ情報 4 0 は、ユーザ 1 0 がコンピュータプログラムにセキュリティホールを発見した場合に、当該コンピュータプログラムの開発元へ提供される情報である。

【 0 0 2 1 】

具体的には、図 2 (a) に示したセキュリティ情報 4 0 は、「登録者」(ユーザ 1 0) および「セキュリティ情報の内容」(ソフトウェア X のバグ問題) から構成されている。「登録者」は、当該セキュリティ情報を登録した者を表す情報であり、「セキュリティ情報の内容」は、当該セキュリティ情報の具体的内容を表す情報である。

【 0 0 2 2 】

返答情報 4 1 A は、セキュリティ情報 4 0 が有効であると開発元に判断された場合に、当該開発元からユーザ 1 0 へ返答される情報である。具体的には、図 2 (b) に示した返答情報 4 1 A は、「返答者」(開発元 3 1 A)、「判定結果」(有効)、「登録者」(ユーザ 1 0) および「セキュリティ情報の内容」(ソフトウェア X のバグ問題) から構成されている。

【 0 0 2 3 】

「返答者」は、セキュリティ情報仲介装置 2 0 に登録されたセキュリティ情報に対して返答した開発元を表す情報である。「判定結果」は、当該セキュリティ

情報が有効であるか否かの結果を表す情報である。「登録者」は、当該セキュリティ情報を登録した者を表す情報であり、「セキュリティ情報の内容」は、当該セキュリティ情報の具体的内容を表す情報である。

【 0 0 2 4 】

支払情報 4 2 は、開発元 3 1 A 側でセキュリティ情報 4 0 が有効であると判定された場合に、セキュリティ情報 4 0 を提供した代償として、開発元 3 1 A からユーザ 1 0 へ支払われる金額や、支払い方法等に関する情報である。具体的には、図 2 (d) に示した支払情報 4 2 は、「支払金額」(1 0 0 0 0 円)、「支払先」(ユーザ 1 0)、「支払者」(開発元 3 1 A) および「支払方法」(電子決済) から構成されている。

【 0 0 2 5 】

「支払金額」は、セキュリティ情報 4 0 を提供した代償として開発元 3 1 A からユーザ 1 0 へ支払われる金額を表す情報である。「支払先」は、上記金額の支払い先を表す情報である。「支払者」は、上記金額を支払う者を表す情報である。「支払方法」は、上記金額を支払者に支払う方法を表す情報である。なお、実施の形態 1 では、「支払方法」として電子決済を一例としているが、金融機関口座への振り込み等、他の支払い方法を用いてもよい。

【 0 0 2 6 】

セキュリティ情報仲介装置 2 0 は、ユーザ 1 0 と開発元 3 1 A および 3 1 B との間においてセキュリティ情報を仲介するサーバであり、ネットワーク 1 2 とネットワーク 3 2 との間に介挿されている。このセキュリティ情報仲介装置 2 0 には、ユーザクライアント 1 1、開発元クライアント 3 0 A および 3 0 B がアクセスする。

【 0 0 2 7 】

セキュリティ情報仲介装置 2 0 において、セキュリティ情報登録部 2 1 は、ユーザクライアント 1 1 からのセキュリティ情報 4 0 をセキュリティ情報データベース 2 2 に登録する機能を備えている。なお、実際には、ネットワーク 1 2 には、ユーザクライアント 1 1 以外に多数のユーザクライアントが接続されている。従って、セキュリティ情報登録部 2 1 は、他のユーザクライアントからのセキュ

リティ情報をセキュリティ情報データベース22に登録する機能も備えている。

【0028】

転送部23は、セキュリティ情報登録部21により登録されたセキュリティ情報を、ネットワーク32を介して開発元クライアント30Aおよび30Bに転送する機能を備えている。ネットワーク32は、セキュリティ情報仲介装置20と開発元クライアント30Aおよび30Bとを接続するものである。開発元クライアント30Aは、コンピュータプログラムのベンダである開発元31A側に設置されたコンピュータ端末である。開発元クライアント30Bは、コンピュータプログラムのベンダである開発元31B側に設置されたコンピュータ端末である。

【0029】

開発元クライアント30Aは、転送部23からのセキュリティ情報40を受信し、上述した返答情報41A（図2（b）参照）および支払情報42（図2（d）参照）をセキュリティ情報仲介装置20へ送信する。同様にして、開発元クライアント30Bは、転送部23からのセキュリティ情報40を受信し、返答情報41Bをセキュリティ情報仲介装置20へ送信する。

【0030】

同図に示した例では、開発元クライアント30Bからは、支払情報が送信されない。これは、セキュリティ情報40が開発元31Bにとって無効であり、代償としての支払いが発生しないからである。つまり、返答情報41A（図2（b）参照）の「判定結果」が有効であるのに対して、返答情報41B（図2（c）参照）の「判定結果」は、無効である。この場合、返答情報41Bの「返答者」は、開発元31Bとされている。

【0031】

セキュリティ情報仲介装置20において、返答情報登録部24は、開発元クライアント30Aおよび開発元クライアント30Bからネットワーク32を介して送信される返答情報41A、支払情報42および返答情報41Bを返答情報データベース25に登録する機能を備えている。転送部26は、返答情報登録部24に登録された返答情報のうち「判定結果」が有効とされた返答情報（同図では返答情報41A）と、該返答情報に対応する支払情報（同図では支払情報42）と

を、ネットワーク 1 2 を介して当該ユーザクライアント（同図ではユーザクライアント 1 1）に転送する機能を備えている。

【 0 0 3 2 】

つぎに、実施の形態 1 の動作について、図 3 に示したフローチャートを参照しつつ説明する。同図に示したステップ S A 1 では、セキュリティ情報登録部 2 1 は、ユーザクライアント 1 1 からセキュリティ情報を受信したか否かを判断し、この場合、判断結果を「N o」として同判断を繰り返す。ここで、ソフトウェア X のバグ（セキュリティホール）を発見したユーザ 1 0 は、図 2（a）に示したセキュリティ情報 4 0 をユーザクライアント 1 1 により作成する。つぎに、ユーザ 1 0 の操作により、ユーザクライアント 1 1 からセキュリティ情報仲介装置 2 0 へセキュリティ情報 4 0 が送信される。

【 0 0 3 3 】

そして、上記セキュリティ情報 4 0 を受信すると、セキュリティ情報登録部 2 1 は、ステップ S A 1 の判断結果を「Y e s」とする。ステップ S A 2 では、セキュリティ情報登録部 2 1 は、セキュリティ情報 4 0 をセキュリティ情報データベース 2 2 に登録する。ステップ S A 3 では、セキュリティ情報登録部 2 1 は、セキュリティ情報 4 0 を転送部 2 3 へ渡す。これにより、転送部 2 3 は、セキュリティ情報 4 0 を開発元クライアント 3 0 A および 3 0 B に並列的に転送する。ステップ S A 4 では、返答情報登録部 2 4 は、返答情報を受信したか否かを判断し、この場合、判断結果を「N o」として同判断を繰り返す。

【 0 0 3 4 】

そして、開発元クライアント 3 0 A および 3 0 B によりセキュリティ情報 4 0 がそれぞれ受信されると、開発元 3 1 A および 3 1 B は、セキュリティ情報 4 0 が有効な情報であるか否かをそれぞれ判断する。ここで「有効」とは、セキュリティ情報 4 0 が、当該ソフトウェア X のバージョンアップに貢献し、かつ提供の代償としてユーザ 1 0 に対して所定の金額を支払うことが妥当であると判断された状態をいう。

【 0 0 3 5 】

この場合、開発元 3 1 A では、セキュリティ情報 4 0 が有効であると判断され

たものとする。開発元31Aでは、開発元クライアント30Aを用いて、返答情報41A（図2（b）参照）および支払情報42（図2（d）参照）を作成した後、これらをセキュリティ情報仲介装置20宛に送信する。これらの返答情報41Aおよび支払情報42は、ネットワーク32を介してセキュリティ情報仲介装置20の返答情報登録部24に受信される。

【0036】

これにより、返答情報登録部24は、ステップSA4の判断結果を「Yes」とする。ステップSA5では、返答情報登録部24は、図2（b）に示した返答情報41Aの「判定結果」が有効であるか否かを判断し、この場合、判断結果を「Yes」とする。ステップSA6では、返答情報登録部24は、受信した返答情報41Aに対応する支払情報を受信したか否かを判断し、この場合、判断結果を「Yes」とする。なお、ステップSA6の判断結果が「No」である場合、返答情報登録部24は、同判断を繰り返す。

【0037】

ステップSA7では、返答情報登録部24は、返答情報41Aおよび支払情報42を返答情報データベース25に登録する。ステップSA8では、返答情報登録部24は、返答情報41Aおよび支払情報42を転送部26へ渡す。これにより、転送部26は、返答情報41Aおよび支払情報42をネットワーク12を介してユーザクライアント11へ転送する。

【0038】

これらの返答情報41Aおよび支払情報42がユーザクライアント11に受信されると、ユーザクライアント11は、返答情報41Aおよび支払情報42をユーザ10に報知する。これにより、ユーザ10は、自身が提供したセキュリティ情報40が有用であったことを認識するとともに、電子決済により開発元31Aから10000円が支払われることを認識する。

【0039】

一方、開発元31Bでは、セキュリティ情報40が無効な情報であると判断したものとする。ここでいう「無効」とは、当該ソフトウェアXが開発元31Bと無関係であって、かつ提供の代償としてユーザに対して所定の金額を支払う必要

がない状態をいう。この場合、開発元 3 1 B では、開発元クライアント 3 0 B を用いて、無効である旨の返答情報 4 1 B（図 2（c）参照）を作成した後、これをセキュリティ情報仲介装置 2 0 宛に送信する。この返答情報 4 1 B は、ネットワーク 3 2 を介してセキュリティ情報仲介装置 2 0 の返答情報登録部 2 4 に受信される。

【0040】

これにより、返答情報登録部 2 4 は、ステップ S A 4 の判断結果を「Y e s」とする。ステップ S A 5 では、返答情報登録部 2 4 は、図 2（c）に示した返答情報 4 1 B の「判定結果」が有効であるか否かを判断し、この場合、判断結果を「N o」とする。ステップ S A 9 では、返答情報 4 1 B を返答情報データベース 2 5 に登録する。

【0041】

以上説明したように、実施の形態 1 によれば、ユーザ 1 0 からのセキュリティ情報 4 0 をダイレクトに開発元 3 1 A および開発元 3 1 B に提供し、しかも有用なセキュリティ情報を提供した者に対して支払いを行うようにしたので、ユーザ 1 0 にとってセキュリティ情報を提供し易い環境を整備し、開発元 3 1 A および開発元 3 1 B にとって低コストで有用なセキュリティ情報を収集することができる。

【0042】

（実施の形態 2）

図 4 は、本発明にかかる実施の形態 2 の構成を示すブロック図である。この図において、ユーザクライアント 1 0 1 A は、ユーザ 1 0 0 A により操作されるコンピュータ端末であり、ネットワーク 1 0 2 を介してセキュリティ情報仲介装置 2 0 0 にアクセス可能とされている。ユーザ 1 0 0 A は、後述する開発元 3 0 1、その他の開発元により開発された各種コンピュータプログラムを利用する者である。また、ユーザ 1 0 0 A は、コンピュータプログラムのバグ等のセキュリティホールを発見し、これをセキュリティ情報として提供することができる知識を有するものである。

【0043】

また、ユーザクライアント101Aは、ユーザクライアント11（図1参照）と同様にして、ネットワーク102を介してセキュリティ情報仲介装置200にセキュリティ情報400Aを登録する機能と、セキュリティ情報仲介装置200からの情報（同図では、返答情報401Aおよび支払情報402）を受信する機能とを備えている。

【0044】

上記セキュリティ情報400Aは、ユーザ100Aがコンピュータプログラムにセキュリティホールを発見した場合に、当該コンピュータプログラムの開発元へ提供される情報であり、セキュリティ情報40（図2（a）参照）と同一の構成とされている。具体的には、図5（a）に示したセキュリティ情報400Aは、「登録者」（ユーザ100A）および「セキュリティ情報の内容」（ソフトウェアXのバグ問題QA）から構成されている。

【0045】

返答情報401Aは、返答情報41A（図2（b）参照）と同様にして、セキュリティ情報400Aが有効であると開発元に判断された場合に、当該開発元からユーザ100Aへ返答される情報である。具体的には、図5（c）に示した返答情報401Aは、「返答者」（開発元301）、「判定結果」（有効）、「登録者」（ユーザ100A）および「セキュリティ情報の内容」（ソフトウェアXのバグ問題QA）から構成されている。

【0046】

支払情報402は、支払情報42（図2（d）参照）と同様にして、開発元301側でセキュリティ情報400Aが有効であると判断された場合に、セキュリティ情報400Aを提供した代償として、開発元301からユーザ100Aへ支払われる金額や、支払い方法等に関する情報である。具体的には、図5（e）に示した支払情報402は、「支払金額」（10000円）、「支払先」（ユーザ100A）、「支払者」（開発元301）および「支払方法」（電子決済）から構成されている。

【0047】

一方、ユーザクライアント101Bは、ユーザ100Bにより操作されるコン

ピュータ端末であり、ネットワーク102を介してセキュリティ情報仲介装置200にアクセス可能とされている。ユーザ100Bは、ユーザ100Aと同様に、開発元301、その他の開発元により開発された各種コンピュータプログラムを利用する者である。また、ユーザ100Bは、コンピュータプログラムのバグ等のセキュリティホールを発見し、これをセキュリティ情報として提供することができる知識を有するものである。

【0048】

また、ユーザクライアント101Bは、ユーザクライアント101Aと同様に、ネットワーク102を介してセキュリティ情報仲介装置200にセキュリティ情報400Bを登録する機能と、セキュリティ情報仲介装置200からの情報（同図では返答情報401B）を受信する機能とを備えている。

【0049】

このセキュリティ情報400Bは、ユーザ100Bがコンピュータプログラムにセキュリティホールを発見した場合に、当該コンピュータプログラムの開発元へ提供される情報であり、セキュリティ情報40（図2（a）参照）と同一の構成とされている。具体的には、図5（b）に示したセキュリティ情報400Bは、「登録者」（ユーザ100B）および「セキュリティ情報の内容」（ソフトウェアXのバグ問題QB）から構成されている。

【0050】

返答情報401Bは、セキュリティ情報400Bが無効であると開発元に判断された場合に、当該開発元からユーザ100Bへ返答される情報である。具体的には、図5（d）に示した返答情報401Bは、「返答者」（開発元301）、「判定結果」（無効）、「登録者」（ユーザ100B）および「セキュリティ情報の内容」（ソフトウェアXのバグ問題QB）から構成されている。

【0051】

セキュリティ情報仲介装置200は、ユーザ100Aおよび100Bと開発元301との間においてセキュリティ情報を仲介するサーバであり、ネットワーク102とネットワーク302との間に介挿されている。このセキュリティ情報仲介装置200には、ユーザクライアント101A、101B、開発元クライアン

ト 3 0 0 がアクセスする。

【 0 0 5 2 】

セキュリティ情報仲介装置 2 0 0 において、受信部 2 0 1 は、ユーザクライアント 1 0 1 A および 1 0 1 B からのセキュリティ情報 4 0 0 A および 4 0 0 B を受信する機能を備えている。情報管理部 2 0 2 は、受信部 2 0 1 に受信されたセキュリティ情報 4 0 0 A および 4 0 0 B や、後述する受信部 2 0 6 に受信された返答情報 4 0 1 A、4 0 1 B および支払情報 4 0 2 を管理する機能を備えている。この情報管理部 2 0 2 の機能については、後述する。

【 0 0 5 3 】

転送部 2 0 5 は、情報管理部 2 0 2 により登録されたセキュリティ情報を、ネットワーク 3 0 2 を介して開発元クライアント 3 0 0 に転送する機能を備えている。ネットワーク 3 0 2 は、セキュリティ情報仲介装置 2 0 0 と開発元クライアント 3 0 0 とを接続するものである。開発元クライアント 3 0 0 は、コンピュータプログラムのベンダである開発元 3 0 1 側に設置されたコンピュータ端末である。

【 0 0 5 4 】

開発元クライアント 3 0 0 は、転送部 2 0 5 からのセキュリティ情報 4 0 0 A および 4 0 0 B を受信し、上述した返答情報 4 0 1 A (図 5 (c) 参照)、返答情報 4 0 1 B (図 5 (d) 参照) および支払情報 4 0 2 (図 5 (e) 参照) をセキュリティ情報仲介装置 2 0 0 へ送信する。

【 0 0 5 5 】

同図に示した例では、開発元クライアント 3 0 0 からは、セキュリティ情報 4 0 0 B に対応する支払情報が送信されない。これは、セキュリティ情報 4 0 0 B が開発元 3 0 1 にとって無効であり、代償としての支払いが発生しないからである。つまり、返答情報 4 0 1 A (図 5 (c) 参照) の「判定結果」が有効であるのに対して、返答情報 4 0 1 B (図 5 (d) 参照) の「判定結果」は、無効である。この場合、返答情報 4 0 1 A および 4 0 1 B のそれぞれの「返答者」は、共に開発元 3 0 1 とされている。

【 0 0 5 6 】

セキュリティ情報仲介装置200において、受信部206は、開発元クライアント300からネットワーク302を介して送信される返答情報、支払情報（同図では、返答情報401A、401B、支払情報402）を受信する機能を備えている。情報管理部202は、受信部201に受信されたセキュリティ情報（同図では、セキュリティ情報400Aおよび400B）を図6（a）に示したセキュリティ情報データベース203に登録する機能を備えている。

【0057】

このセキュリティ情報データベース203は、セキュリティ情報に対して登録順に付与される「登録番号」、「登録日時」、「登録者」および「セキュリティ情報の内容」から構成されている。同図において、「登録番号」=「3」のレコードは、セキュリティ情報400A（図5（a）参照）に対応しており、「登録番号」=「4」のレコードは、セキュリティ情報400B（図5（b）参照）に対応している。

【0058】

また、情報管理部202は、受信部206に受信された返答情報（同図では、返答情報401Aおよび401B）を図6（b）に示した返答情報データベース204に登録する機能を備えている。この返答情報データベース204は、返答情報に対して登録順に付与される「返答番号」、「返答日時」、「登録番号」（図6（a）参照）、「返答者」および「判定結果」から構成されている。同図において、「返答番号」=「3」のレコードは、返答情報401A（図5（c）参照）に対応しており、「返答番号」=「4」のレコードは、返答情報401B（図5（d）参照）に対応している。

【0059】

さらに、情報管理部202は、「判定結果」が「有効」または「無効」とされた返答情報（同図では返答情報401Aおよび返答情報401B）と、支払情報（同図では支払情報402）とを転送部207へ渡す。転送部207は、情報管理部202からの返答情報、支払情報を当該ユーザクライアントへネットワーク102を介して転送する機能を備えている。

【0060】

つぎに、実施の形態2の動作について、図7に示したフローチャートを参照しつつ説明する。同図に示したステップSB1では、情報管理部202は、受信部201によりセキュリティ情報が受信されたか否かを判断し、この場合、判断結果を「No」として同判断を繰り返す。

【0061】

ここで、ソフトウェアXのバグ（セキュリティホール）を発見したユーザ100Aは、図5（a）に示したセキュリティ情報400Aをユーザクライアント101Aにより作成する。つぎに、ユーザ100Aの操作により、ユーザクライアント101Aからセキュリティ情報仲介装置200へセキュリティ情報400Aが送信される。

【0062】

そして、上記セキュリティ情報400Aが受信部201に受信されると、情報管理部202は、ステップSB1の判断結果を「Yes」とする。ステップSB2では、情報管理部202は、セキュリティ情報400Aの「登録者」および「セキュリティ情報の内容」をキーとして、図6（a）に示したセキュリティ情報データベース203を検索する。この場合、セキュリティ情報データベース203には、「登録番号」=1および2のレコードのみが存在しているものとする。

【0063】

ステップSB3では、情報管理部202は、検索ヒットしたか否か、すなわち、セキュリティ情報400Aと同一の内容がセキュリティ情報データベース203に登録されているか否かを判断し、この判断結果が「Yes」である場合、ステップSB11では、情報管理部202は、登録拒絶をする。この場合、情報管理部202は、ステップSB3の判断結果を「No」とする。

【0064】

ステップSB4では、情報管理部202は、セキュリティ情報400Aをセキュリティ情報データベース203（図6（a）参照）に登録する。これにより、セキュリティ情報データベース203には、「登録番号」=3のレコード（セキュリティ情報400Aに対応）が追加される。

【0065】

ステップSB5では、情報管理部202は、上記セキュリティ情報400Aを転送部205へ渡す。これにより、転送部205は、セキュリティ情報400Aをネットワーク302を介して開発元クライアント300に転送する。ステップSB6では、情報管理部202は、受信部206により返答情報が受信されたか否かを判断し、この場合、判断結果を「No」として同判断を繰り返す。

【0066】

そして、開発元クライアント300によりセキュリティ情報400Aが受信されると、開発元301は、セキュリティ情報400Aが有効な情報であるか否かを判断する。この場合、開発元301では、セキュリティ情報400Aが有効であると判断されたものとする。開発元301では、開発元クライアント300を用いて、返答情報401A（図5（c）参照）および支払情報402（図5（e）参照）を作成した後、これらをセキュリティ情報仲介装置200宛に送信する。これらの返答情報401Aおよび支払情報402は、ネットワーク302を介してセキュリティ情報仲介装置200の受信部206に受信される。

【0067】

これにより、情報管理部202は、ステップSB6の判断結果を「Yes」とする。ステップSB7では、情報管理部202は、返答情報401Aを返答情報データベース204（図6（b）参照）に登録する。これにより、返答情報データベース204には、「返答番号」=3のレコード（返答情報401Aに対応）が追加される。

【0068】

ステップSB8では、情報管理部202は、図5（c）に示した返答情報401Aの「判定結果」が有効であるか否かを判断し、この場合、判断結果を「Yes」とする。ステップSB9では、情報管理部202は、返答情報401Aに対応する支払情報402が受信部206に受信されたか否かを判断し、この場合、判断結果を「Yes」とする。なお、ステップSB9の判断結果が「No」である場合、情報管理部202は、同判断を繰り返す。

【0069】

ステップSB10では、情報管理部202は、返答情報401Aおよび支払情

報402を転送部207へ渡す。これにより、転送部207は、返答情報401 Aおよび支払情報402をネットワーク102を介してユーザクライアント101 Aへ転送する。

【0070】

これらの返答情報401 Aおよび支払情報402がユーザクライアント101 Aに受信されると、ユーザクライアント101 Aは、返答情報401 Aおよび支払情報402をユーザ100 Aに報知する。これにより、ユーザ100 Aは、自身が提供したセキュリティ情報400 Aが有用であったことを認識するとともに、電子決済により開発元301から10000円が支払われることを認識する。

【0071】

一方、ソフトウェアXのバグ（セキュリティホール）を発見したユーザ100 Bは、図5（b）に示したセキュリティ情報400 Bをユーザクライアント101 Bにより作成する。つぎに、ユーザ100 Bの操作により、ユーザクライアント101 Bからセキュリティ情報仲介装置200へセキュリティ情報400 Bが送信される。

【0072】

そして、上記セキュリティ情報400 Bが受信部201に受信されると、情報管理部202は、ステップSB1の判断結果を「Yes」とする。ステップSB2では、情報管理部202は、セキュリティ情報400 Bの「登録者」および「セキュリティ情報の内容」をキーとして、セキュリティ情報データベース203を検索する。この場合、セキュリティ情報データベース203には、「登録番号」=1～3のレコードのみが存在しているものとする。

【0073】

ステップSB3では、情報管理部202は、検索ヒットしたか否かを判断し、この場合、判断結果を「No」とする。ステップSB4では、情報管理部202は、セキュリティ情報400 Bをセキュリティ情報データベース203（図6（a）参照）に登録する。これにより、セキュリティ情報データベース203には、「登録番号」=4のレコード（セキュリティ情報400 Bに対応）が追加される。

【 0 0 7 4 】

ステップ S B 5 では、情報管理部 2 0 2 は、上記セキュリティ情報 4 0 0 B を転送部 2 0 5 へ渡す。これにより、転送部 2 0 5 は、セキュリティ情報 4 0 0 B をネットワーク 3 0 2 を介して開発元クライアント 3 0 0 に転送する。ステップ S B 6 では、情報管理部 2 0 2 は、受信部 2 0 6 により返答情報が受信されたか否かを判断し、この場合、判断結果を「N o」そして同判断を繰り返す。

【 0 0 7 5 】

そして、開発元クライアント 3 0 0 によりセキュリティ情報 4 0 0 B が受信されると、開発元 3 0 1 は、セキュリティ情報 4 0 0 B が有効な情報であるか否かを判断する。この場合、開発元 3 0 1 では、セキュリティ情報 4 0 0 B が無効であると判断されたものとする。開発元 3 0 1 では、開発元クライアント 3 0 0 を用いて、拒絶メッセージとしての返答情報 4 0 1 B（図 5（d）参照）を作成した後、これをセキュリティ情報仲介装置 2 0 0 宛に送信する。

【 0 0 7 6 】

そして、返答情報 4 0 1 B は、ネットワーク 3 0 2 を介してセキュリティ情報仲介装置 2 0 0 の受信部 2 0 6 に受信される。これにより、情報管理部 2 0 2 は、ステップ S B 6 の判断結果を「Y e s」とする。ステップ S B 7 では、情報管理部 2 0 2 は、返答情報 4 0 1 B を返答情報データベース 2 0 4（図 6（b）参照）に登録する。これにより、返答情報データベース 2 0 4 には、「返答番号」= 4 のレコード（返答情報 4 0 1 B に対応）が追加される。

【 0 0 7 7 】

ステップ S B 8 では、情報管理部 2 0 2 は、図 5（d）に示した返答情報 4 0 1 B の「判定結果」が有効であるか否かを判断し、この場合、判断結果を「N o」とする。ステップ S B 1 2 では、情報管理部 2 0 2 は、拒絶メッセージとしての返答情報 4 0 1 B を転送部 2 0 7 へ渡す。これにより、転送部 2 0 7 は、返答情報 4 0 1 B をネットワーク 1 0 2 を介してユーザクライアント 1 0 1 B へ転送する。この返答情報 4 0 1 B がユーザクライアント 1 0 1 B に受信されると、ユーザクライアント 1 0 1 B は、返答情報 4 0 1 B をユーザ 1 0 0 B に報知する。これにより、ユーザ 1 0 0 B は、自身が提供したセキュリティ情報 4 0 0 B が無

効であったことを認識する。

【 0 0 7 8 】

以上説明したように、実施の形態 2 によれば、ユーザ 1 0 0 B から提供されたセキュリティ情報 4 0 0 B の無効を示す返答情報 4 0 1 B をユーザクライアント 1 0 1 B へ転送するようにしたので、提供したセキュリティ情報の使われ方（有用または無効）に関心を持つユーザに対するサービスを向上させることができる。

【 0 0 7 9 】

また、実施の形態 2 によれば、ユーザ（ユーザ 1 0 0 A、1 0 0 B）より提供されたセキュリティ情報（セキュリティ情報 4 0 0 A、4 0 0 B）が新規である場合にのみ、当該セキュリティ情報を開発元クライアント 3 0 0 へ転送するようにしたので、不要なセキュリティ情報を開発元クライアント 3 0 0 へ転送するという無駄を防止でき、効率良くセキュリティ情報の収集を行うことができる。

【 0 0 8 0 】

（実施の形態 3）

図 8 は、本発明にかかる実施の形態 3 の構成を示すブロック図である。この図において、ユーザクライアント 5 0 1 は、ユーザ 5 0 0 により操作されるコンピュータ端末であり、ネットワーク 5 0 2 を介してセキュリティ情報仲介装置 6 0 0 にアクセス可能とされている。

【 0 0 8 1 】

ユーザ 5 0 0 は、後述する開発元 7 0 1 A および 7 0 1 B、その他の開発元により開発された各種コンピュータプログラムを利用する者である。また、ユーザ 5 0 0 は、コンピュータプログラムのバグ等のセキュリティホールを発見し、これをセキュリティ情報として提供することができる知識を有するものである。

【 0 0 8 2 】

また、ユーザクライアント 5 0 1 は、ユーザクライアント 1 1（図 1 参照）と同様にして、ネットワーク 5 0 2 を介してセキュリティ情報仲介装置 6 0 0 にセキュリティ情報 8 0 0 を登録する機能と、セキュリティ情報仲介装置 6 0 0 からの情報（同図では、返答情報 8 0 1 および支払情報 8 0 2）を受信する機能とを

備えている。

【0083】

上記セキュリティ情報800は、ユーザ500がコンピュータプログラムにセキュリティホールを発見した場合に、当該コンピュータプログラムの開発元へ提供される情報であり、セキュリティ情報40（図2（a）参照）と同一の構成とされている。具体的には、図9（a）に示したセキュリティ情報800は、「登録者」（ユーザ500）および「セキュリティ情報の内容」（ソフトウェアXのバグ問題）から構成されている。

【0084】

返答情報801は、返答情報41A（図2（b）参照）と同様にして、セキュリティ情報800が有効であると開発元に判断された場合に、当該開発元からユーザ500へ返答される情報である。具体的には、図9（b）に示した返答情報801は、「返答者」（開発元701A）、「判定結果」（有効）、「登録者」（ユーザ500）、「分類」（A）および「セキュリティ情報の内容」（ソフトウェアXのバグ問題）から構成されている。上記「分類」は、当該セキュリティ情報の内容が該当する分類項目を表す情報である。

【0085】

支払情報802は、支払情報42（図2（d）参照）と同様にして、開発元701A側でセキュリティ情報800が有効であると判断された場合に、セキュリティ情報800を提供した代償として、開発元701Aからユーザ500へ支払われる金額や、支払い方法等に関する情報である。具体的には、図9（c）に示した支払情報802は、「支払金額」（10000円）、「支払先」（ユーザ500）、「支払者」（開発元701A）および「支払方法」（電子決済）から構成されている。

【0086】

セキュリティ情報仲介装置600は、ユーザ500と、開発元701Aおよび701Bとの間においてセキュリティ情報を仲介するサーバであり、ネットワーク502とネットワーク702との間に介挿されている。このセキュリティ情報仲介装置600には、ユーザクライアント501、開発元クライアント700A

および 7 0 0 B がアクセスする。

【 0 0 8 7 】

セキュリティ情報仲介装置 6 0 0 において、受信部 6 0 1 は、ユーザクライアント 5 0 1 からのセキュリティ情報 8 0 0 を受信する機能を備えている。情報管理部 6 0 2 は、受信部 6 0 1 に受信されたセキュリティ情報 8 0 0 や、後述する受信部 6 0 7 に受信された返答情報 8 0 1 および支払情報 8 0 2 を管理する機能を備えている。この情報管理部 6 0 2 の機能については、後述する。

【 0 0 8 8 】

転送部 6 0 5 は、情報管理部 6 0 2 により登録されたセキュリティ情報を、ネットワーク 7 0 2 を介して開発元クライアント 7 0 0 A および 7 0 0 B の双方に転送する機能を備えている。また、転送部 6 0 5 は、開発元クライアント 7 0 0 A および 7 0 0 B からの分類情報 8 0 3 A および 8 0 3 B を受信し、これらを分類情報データベース 6 0 6 に登録する機能も備えている。

【 0 0 8 9 】

分類情報 8 0 3 A は、開発元 7 0 1 A で必要とするセキュリティ情報の分類を表す情報である。具体的には、図 9 (d) に示した分類情報 8 0 3 A は、「開発元」(開発元 7 0 1 A) および「分類」(A) から構成されている。従って、開発元 7 0 1 A は、分類「 A 」に属するセキュリティ情報のみが必要であって、その他の分類に属するセキュリティ情報を必要としていない。つまり、分類情報 8 0 3 A は、セキュリティ情報仲介装置 6 0 0 に登録される多数のセキュリティ情報の中から、開発元 7 0 1 A で必要とするセキュリティ情報を抽出するためのフィルタリング情報である。

【 0 0 9 0 】

一方、分類情報 8 0 3 B は、分類情報 8 0 3 A と同様にして、開発元 7 0 1 B で必要とするセキュリティ情報の分類を表す情報である。具体的には、図 9 (e) に示した分類情報 8 0 3 B は、「開発元」(開発元 7 0 1 B) および「分類」(B) から構成されている。

【 0 0 9 1 】

従って、開発元 7 0 1 B は、分類「 B 」に属するセキュリティ情報のみが必要

であって、その他の分類に属するセキュリティ情報を必要としていない。このように、分類情報 8 0 3 B も、分類情報 8 0 3 A と同様にして、セキュリティ情報仲介装置 6 0 0 に登録される多数のセキュリティ情報の中から、開発元 7 0 1 B で必要とするセキュリティ情報を抽出するためのフィルタリング情報である。

【 0 0 9 2 】

また、分類情報データベース 6 0 6 は、図 1 0 (c) に示したように、「開発元」および「分類」から構成されている。この分類情報データベース 6 0 6 において、「開発元」 (= 開発元 7 0 1 A) のレコードは、分類情報 8 0 3 A (図 9 (d) 参照) に対応しており、「開発元」 (= 開発元 7 0 1 B) のレコードは、分類情報 8 0 3 B (図 9 (e) 参照) に対応している。

【 0 0 9 3 】

ネットワーク 7 0 2 は、セキュリティ情報仲介装置 6 0 0 と開発元クライアント 7 0 0 A および 7 0 0 B とを接続するものである。開発元クライアント 7 0 0 A は、コンピュータプログラムのベンダである開発元 7 0 1 A 側に設置されたコンピュータ端末である。開発元クライアント 7 0 0 B は、コンピュータプログラムのベンダである開発元 7 0 1 B 側に設置されたコンピュータ端末である。

【 0 0 9 4 】

開発元クライアント 7 0 0 A は、分類情報 8 0 3 A (図 9 (d) 参照) を転送部 6 0 5 へ送信し、また、上記分類情報 8 0 3 A に対応するセキュリティ情報 (同図では、セキュリティ情報 8 0 0) を受信する。また、開発元クライアント 7 0 0 A は、当該セキュリティ情報が有効である場合、上述した返答情報 8 0 1 (図 9 (b) 参照) および支払情報 8 0 2 (図 9 (c) 参照) をセキュリティ情報仲介装置 6 0 0 へ送信する。

【 0 0 9 5 】

一方、開発元クライアント 7 0 0 B は、分類情報 8 0 3 B (図 9 (e) 参照) を転送部 6 0 5 へ送信し、また、上記分類情報 8 0 3 B に対応するセキュリティ情報を受信する。また、開発元クライアント 7 0 0 B は、開発元クライアント 7 0 0 A と同様にして、当該セキュリティ情報が有効である場合、返答情報および支払情報をセキュリティ情報仲介装置 6 0 0 へ送信する。

【 0 0 9 6 】

セキュリティ情報仲介装置 6 0 0 において、受信部 6 0 7 は、開発元クライアント 7 0 0 A、7 0 0 B からネットワーク 7 0 2 を介して送信される返答情報、支払情報（同図では、返答情報 8 0 1 および支払情報 8 0 2）を受信する機能を備えている。情報管理部 6 0 2 は、受信部 6 0 1 に受信されたセキュリティ情報（同図では、セキュリティ情報 8 0 0）を図 1 0（a）に示したセキュリティ情報データベース 6 0 3 に登録する機能を備えている。

【 0 0 9 7 】

このセキュリティ情報データベース 6 0 3 は、セキュリティ情報に対して登録順に付与される「登録番号」、「登録日時」、「登録者」、セキュリティ情報の分類を表す「分類」、および「セキュリティ情報の内容」から構成されている。同図において、「登録番号」＝「3」のレコードは、セキュリティ情報 8 0 0（図 9（a）参照）に対応している。

【 0 0 9 8 】

また、情報管理部 6 0 2 は、受信部 6 0 7 に受信された返答情報（同図では、返答情報 8 0 1）を図 1 0（b）に示した返答情報データベース 6 0 4 に登録する機能を備えている。この返答情報データベース 6 0 4 は、返答情報に対して登録順に付与される「返答番号」、「返答日時」、「登録番号」（図 1 0（a）参照）、「返答者」、「分類」（図 1 0（a）参照）および「判定結果」から構成されている。同図において、「返答番号」＝「3」のレコードは、返答情報 8 0 1（図 9（b）参照）に対応している。

【 0 0 9 9 】

さらに、情報管理部 6 0 2 は、「判定結果」が「有効」または「無効」とされた返答情報（同図では返答情報 8 0 1）と、支払情報（同図では支払情報 8 0 2）とを転送部 6 0 8 へ渡す。転送部 6 0 8 は、情報管理部 6 0 2 からの返答情報、支払情報を当該ユーザクライアントへネットワーク 5 0 2 を介して転送する機能を備えている。

【 0 1 0 0 】

つぎに、実施の形態 3 の動作について、図 1 1 に示したフローチャートを参照

しつつ説明する。同図に示したステップSC1では、転送部605は、分類情報登録処理を実行する。具体的には、転送部605は、開発元クライアント700Aおよび700Bからネットワーク702を介して、分類情報803A（図9（d）参照）および分類情報803B（図9（e）参照）を受信すると、これらを分類情報データベース606（図10（c）参照）に登録する。

【0101】

上記分類情報登録処理が終了すると、ステップSC2では、情報管理部602は、受信部601によりセキュリティ情報が受信されたか否かを判断し、この場合、判断結果を「No」として同判断を繰り返す。ここで、ソフトウェアXのバグ（セキュリティホール）を発見したユーザ500は、図9（a）に示したセキュリティ情報800をユーザクライアント501により作成する。つぎに、ユーザ500の操作により、ユーザクライアント501からセキュリティ情報仲介装置600へセキュリティ情報800が送信される。

【0102】

そして、上記セキュリティ情報800が受信部601に受信されると、情報管理部602は、ステップSC2の判断結果を「Yes」とする。ステップSC3では、情報管理部602は、セキュリティ情報800の「登録者」および「セキュリティ情報の内容」をキーとして、図10（a）に示したセキュリティ情報データベース603を検索する。この場合、セキュリティ情報データベース603には、「登録番号」=1および2のレコードのみが存在しているものとする。

【0103】

ステップSC4では、情報管理部602は、検索ヒットしたか否か、すなわち、セキュリティ情報800と同一の内容がセキュリティ情報データベース603に登録されているか否かを判断し、この判断結果が「Yes」である場合、ステップSC15では、情報管理部602は、登録拒絶をする。この場合、情報管理部602は、ステップSC4の判断結果を「No」とする。

【0104】

ステップSC5では、情報管理部602は、受信されたセキュリティ情報800の内容に基づいて、当該セキュリティ情報800が、予め設定された分類（例

えば、A～Z)のうち、どの分類に当てはまるかを判断する分類処理を実行する。

【0105】

この場合、情報管理部602は、セキュリティ情報800の分類をAと判断したものとする。ステップSC6では、情報管理部602は、セキュリティ情報800を分類Aに対応付けて、セキュリティ情報データベース603(図10(a)参照)に登録する。これにより、セキュリティ情報データベース603には、「登録番号」=3のレコード(セキュリティ情報800に対応)が追加される。

【0106】

ステップSC7では、情報管理部602は、転送部605を経由して分類情報データベース606にアクセスした後、セキュリティ情報800の分類Aをキーとして図10(c)に示した分類情報データベース606を検索する。ステップSC8では、情報管理部602は、セキュリティ情報800の分類Aと同一の分類が分類情報データベース606に存在するか否かを判断する。

【0107】

この場合、分類情報データベース606における「開発元」(=開発元701A)の分類(=A)がセキュリティ情報800の分類Aと一致しているため、情報管理部602は、ステップSC8の判断結果を「Yes」とする。なお、ステップSC8の判断結果が「No」である場合、情報管理部602は、ステップSC2以降の処理を繰り返す。

【0108】

ステップSC9では、情報管理部602は、開発元クライアント700A宛のセキュリティ情報800を転送部605へ渡す。これにより、転送部605は、セキュリティ情報800を開発元クライアント700Aに転送する。この場合、開発元クライアント700Bには、セキュリティ情報800が転送されない。ステップSC10では、情報管理部602は、受信部607により返答情報が受信されたか否かを判断し、この場合、判断結果を「No」として同判断を繰り返す。

【0109】

そして、開発元クライアント700Aによりセキュリティ情報800が受信されると、開発元701Aは、セキュリティ情報800が有効な情報であるか否かを判断する。この場合、開発元701Aでは、セキュリティ情報800が有効であると判断されたものとする。開発元701Aでは、開発元クライアント700Aを用いて、返答情報801（図9（b）参照）および支払情報802（図9（c）参照）を作成した後、これらをセキュリティ情報仲介装置600宛に送信する。これらの返答情報801および支払情報802は、ネットワーク702を介してセキュリティ情報仲介装置600の受信部607に受信される。

【0110】

これにより、情報管理部602は、ステップSC10の判断結果を「Yes」とする。ステップSC11では、情報管理部602は、返答情報801を返答情報データベース604（図10（b）参照）に登録する。これにより、返答情報データベース604には、「返答番号」=3のレコード（返答情報801に対応）が追加される。

【0111】

ステップSC12では、情報管理部602は、図9（b）に示した返答情報801の「判定結果」が有効であるか否かを判断し、この場合、判断結果を「Yes」とする。ステップSC13では、情報管理部602は、返答情報801に対応する支払情報802が受信部607に受信されたか否かを判断し、この場合、判断結果を「Yes」とする。なお、ステップSC13の判断結果が「No」である場合、情報管理部602は、同判断を繰り返す。

【0112】

ステップSC14では、情報管理部602は、返答情報801および支払情報802を転送部608へ渡す。これにより、転送部608は、返答情報801および支払情報802をネットワーク502を介してユーザクライアント501へ転送する。

【0113】

これらの返答情報801および支払情報802がユーザクライアント501に受信されると、ユーザクライアント501は、返答情報801および支払情報8

02をユーザ500に報知する。これにより、ユーザ500は、自身が提供したセキュリティ情報800が有用であったことを認識するとともに、電子決済により開発元701Aから10000円が支払われることを認識する。

【0114】

一方、ステップSC12の判断結果が「No」である場合、すなわち、「判定結果」＝「無効」の返答情報が受信部607に受信された場合、ステップSC16では、情報管理部602は、拒絶メッセージとしての返答情報を転送部608へ渡す。これにより、転送部608は、返答情報（拒絶メッセージ）をネットワーク502を介してユーザクライアント501へ転送する。この返答情報（拒絶メッセージ）がユーザクライアント501に受信されると、ユーザクライアント501は、該返答情報をユーザ500に報知する。これにより、ユーザ500は、自身が提供したセキュリティ情報が無効であったことを認識する。

【0115】

以上説明したように、実施の形態3によれば、開発元701Aおよび開発元701Bが所望するセキュリティ情報の分類情報を分類情報データベース606に登録しておき、上記分類情報と、ユーザ500から提供されたセキュリティ情報800の分類結果とが一致する場合にのみ当該セキュリティ情報800を例えば開発元クライアント700Aへ転送するようにしたので、不要なセキュリティ情報を転送するという無駄を防止でき、さらに効率良くセキュリティ情報の収集を行うことができる。

【0116】

（実施の形態4）

さて、前述した実施の形態3では、当事者間（ユーザおよび開発元）でセキュリティ情報を共有する例について説明したが、セキュリティ情報や、当該コンピュータプログラムを修正するためのパッチ情報を第三者である一般ユーザに公開するようにしてもよい。以下では、この場合を実施の形態4として説明する。

【0117】

図12は、本発明にかかる実施の形態4の構成を示すブロック図である。この図において、図8の各部に対応する部分には同一の符号を付ける。図12では、

図8に示したセキュリティ情報仲介装置600に代えてセキュリティ情報仲介装置1000が設けられている。

【0118】

このセキュリティ情報仲介装置1000においては、図8に示した情報管理部602および返答情報データベース604に代えて、情報管理部1001および返答情報データベース1002が設けられている。さらに、セキュリティ情報仲介装置1000においては、情報公開部1003および公開情報データベース1004が新たに設けられている。また、図12においては、ユーザ900により操作されるユーザクライアント901が新たに設けられている。

【0119】

セキュリティ情報仲介装置1000は、ユーザ500および900と、開発元701Aおよび701Bとの間においてセキュリティ情報やパッチ情報を仲介するサーバであり、ネットワーク502とネットワーク702との間に介挿されている。このセキュリティ情報仲介装置1000には、ユーザクライアント501、ユーザクライアント901、開発元クライアント700Aおよび700Bがアクセスする。

【0120】

セキュリティ情報仲介装置1000において、受信部607は、前述した返答情報801および支払情報802に加えて、パッチ情報1100を開発元クライアント700Aより受信する。このパッチ情報1100は、図13(c)に示したように、返答情報801に対応する「返答番号」(3)、「返答者」(開発元701A)およびパッチプログラムから構成されており、セキュリティホールを有する当該コンピュータプログラムを修正するための情報である。

【0121】

情報管理部1001は、受信部601に受信されたセキュリティ情報(同図ではセキュリティ情報800)をセキュリティ情報データベース603に登録する機能を備えている。また、情報管理部1001は、受信部607に受信された返答情報(同図では、返答情報801)を図13(a)に示した返答情報データベース1002に登録する機能を備えている。

【0122】

この返答情報データベース1002は、返答情報データベース604（図10（b）参照）と同様にして、返答情報に対して登録順に付与される「返答番号」、「返答日時」、「登録番号」、「返答者」、「分類」および「判定結果」のカラムを備えている。さらに、返答情報データベース1002は、「修正方法」のカラムも備えている。この「修正方法」は、セキュリティホールを有するコンピュータプログラムに対する修正方法（例えば、パッチ）を表す情報である。同図において、「返答番号」＝「3」のレコードは、返答情報801（図9（b）参照）に対応している。

【0123】

また、情報管理部1001は、情報管理部602と同様にして、「判定結果」が「有効」または「無効」とされた返答情報（同図では返答情報801）と、支払情報（同図では支払情報802）とを転送部608へ渡す。さらに、情報管理部1001は、セキュリティ情報、返答情報およびパッチ情報を情報公開部1003へ渡す。

【0124】

情報公開部1003は、webサイト上の情報公開画面1200（図14参照）等を介して、第三者であるユーザ900のユーザクライアント901に対して、セキュリティ情報、返答情報およびパッチ情報を公開する機能を備えている。また、情報公開部1003は、情報管理部1001からの返答情報、セキュリティ情報およびパッチ情報を、図13（b）に示した公開情報データベース1004に登録する。

【0125】

この公開情報データベース1004は、返答情報データベース1002（図13（a）参照）と同様にして、「返答番号」、「分類」、「セキュリティ情報の内容」、「返答者」、「修正方法」、「セキュリティ情報ポインタ」および「パッチ情報ポインタ」から構成されている。「セキュリティ情報ポインタ」は、セキュリティ情報が実際に格納されている領域を表すポインタであり、「パッチ情報ポインタ」は、パッチ情報が実際に格納されている領域を表すポインタである。

【0126】

つぎに、実施の形態4の動作について、図15に示したフローチャートを参照しつつ説明する。同図に示したステップSD1では、転送部605は、ステップSC1（図11参照）と同様にして、分類情報803A（図9（d）参照）および分類情報803B（図9（e）参照）を分類情報データベース606（図10（c）参照）に登録する。

【0127】

ステップSD2では、情報管理部1001は、受信部601によりセキュリティ情報が受信されたか否かを判断し、この場合、判断結果を「No」として同判断を繰り返す。ここで、ソフトウェアXのバグ（セキュリティホール）を発見したユーザ500は、図9（a）に示したセキュリティ情報800をユーザクライアント501により作成する。つぎに、ユーザ500の操作により、ユーザクライアント501からセキュリティ情報仲介装置1000へセキュリティ情報800が送信される。

【0128】

そして、上記セキュリティ情報800が受信部601に受信されると、情報管理部1001は、ステップSD2の判断結果を「Yes」とする。ステップSD3では、情報管理部1001は、セキュリティ情報800の「登録者」および「セキュリティ情報の内容」をキーとして、図10（a）に示したセキュリティ情報データベース603を検索する。この場合、セキュリティ情報データベース603には、「登録番号」=1および2のレコードのみが存在しているものとする。

【0129】

ステップSD4では、情報管理部1001は、検索ヒットしたか否か、すなわち、セキュリティ情報800と同一の内容がセキュリティ情報データベース603に登録されているか否かを判断し、この判断結果が「Yes」である場合、ステップSD19では、情報管理部1001は、登録拒絶をする。この場合、情報管理部1001は、ステップSD4の判断結果を「No」とする。

【0130】

ステップSD5では、情報管理部1001は、受信されたセキュリティ情報800の内容に基づいて、当該セキュリティ情報800が、予め設定された分類（例えば、A～Z）のうち、どの分類に当てはまるかを判断する分類処理を実行する。

【0131】

この場合、情報管理部1001は、セキュリティ情報800の分類をAと判断したものとする。ステップSD6では、情報管理部1001は、セキュリティ情報800を分類Aに対応付けて、セキュリティ情報データベース603（図10（a）参照）に登録する。これにより、セキュリティ情報データベース603には、「登録番号」=3のレコード（セキュリティ情報800に対応）が追加される。また、情報管理部1001は、セキュリティ情報800を情報公開部1003に渡す。これにより、情報公開部1003は、セキュリティ情報800を公開情報データベース1004に登録する。

【0132】

ステップSD7では、情報管理部1001は、転送部605を経由して分類情報データベース606にアクセスした後、セキュリティ情報800の分類Aをキーとして図10（c）に示した分類情報データベース606を検索する。ステップSD8では、情報管理部1001は、セキュリティ情報800の分類Aと同一の分類が分類情報データベース606に存在するか否かを判断する。

【0133】

この場合、分類情報データベース606における「開発元」（＝開発元701A）の分類（＝A）がセキュリティ情報800の分類Aと一致しているため、情報管理部1001は、ステップSD8の判断結果を「Yes」とする。なお、ステップSD4の判断結果が「No」である場合、情報管理部1001は、ステップSD2以降の処理を繰り返す。

【0134】

ステップSD9では、情報管理部1001は、開発元クライアント700A宛のセキュリティ情報800を転送部605へ渡す。これにより、転送部605は

、セキュリティ情報800を開発元クライアント700Aに転送する。この場合、開発元クライアント700Bには、セキュリティ情報800が転送されない。ステップSD10では、情報管理部1001は、受信部607により返答情報が受信されたか否かを判断し、この場合、判断結果を「No」として同判断を繰り返す。

【0135】

そして、開発元クライアント700Aによりセキュリティ情報800が受信されると、開発元701Aは、セキュリティ情報800が有効な情報であるか否かを判断する。この場合、開発元701Aでは、セキュリティ情報800が有効であると判断されたものとする。開発元701Aでは、開発元クライアント700Aを用いて、返答情報801（図9（b）参照）、支払情報802（図9（c）参照）およびパッチ情報1100（図13（c）参照）を作成した後、これらをセキュリティ情報仲介装置1000宛に送信する。これらの返答情報801、支払情報802およびパッチ情報1100は、ネットワーク702を介してセキュリティ情報仲介装置1000の受信部607に受信される。

【0136】

これにより、情報管理部1001は、ステップSD10の判断結果を「Yes」とする。ステップSD11では、情報管理部1001は、受信部607にパッチ情報が受信されたか否かを判断し、この場合、判断結果を「Yes」とする。ステップSD17では、情報管理部1001は、返答情報801およびパッチ情報1100を返答情報データベース1002（図13（a）参照）に登録する。

【0137】

また、情報管理部1001は、返答情報801およびパッチ情報1100を情報公開部1003に渡す。これにより、情報公開部1003は、返答情報801およびパッチ情報1100を公開情報データベース1004（図13（b）参照）に登録する。一方、ステップSD11の判断結果が「No」である場合、情報管理部1001は、返答情報801を返答情報データベース1002（図13（a）参照）に登録する。

【0138】

ステップSD13では、情報管理部1001は、図9(b)に示した返答情報801の「判定結果」が有効であるか否かを判断し、この場合、判断結果を「Yes」とする。ステップSD14では、情報管理部1001は、返答情報801に対応する支払情報802が受信部607に受信されたか否かを判断し、この場合、判断結果を「Yes」とする。なお、ステップSD14の判断結果が「No」である場合、情報管理部1001は、同判断を繰り返す。

【0139】

ステップSD15では、情報管理部1001は、返答情報801および支払情報802を転送部608へ渡す。これにより、転送部608は、返答情報801および支払情報802をネットワーク502を介してユーザクライアント501へ転送する。

【0140】

これらの返答情報801および支払情報802がユーザクライアント501に受信されると、ユーザクライアント501は、返答情報801および支払情報802をユーザ500に報知する。これにより、ユーザ500は、自身が提供したセキュリティ情報800が有用であったことを認識するとともに、電子決済により開発元701Aから10000円が支払われることを認識する。

【0141】

一方、ステップSD13の判断結果が「No」である場合、すなわち、「判定結果」＝「無効」の返答情報が受信部607に受信された場合、ステップSD18では、情報管理部1001は、拒絶メッセージとしての返答情報を転送部608へ渡す。これにより、転送部608は、返答情報（拒絶メッセージ）をネットワーク502を介してユーザクライアント501へ転送する。この返答情報（拒絶メッセージ）がユーザクライアント501に受信されると、ユーザクライアント501は、該返答情報をユーザ500に報知する。これにより、ユーザ500は、自身が提供したセキュリティ情報が無効であったことを認識する。

【0142】

つぎに、図12に示した情報公開部1003の動作について、図16に示したフローチャートを参照しつつ説明する。ステップSE1では、情報公開部100

3は、情報管理部1001からの公開情報（セキュリティ情報、返答情報、パッチ情報）を受信したか否かを判断し、この判断結果が「Yes」である場合、ステップSE2で公開情報データベース1004を更新する。

【0143】

一方、ステップSE1の判断結果が「No」である場合、ステップSE3では、情報公開部1003は、ユーザクライアント（同図ではユーザクライアント901）からアクセス要求があるか否かを判断し、この場合、同判断結果が「No」であるものとする、ステップSE1以降の処理を繰り返す。ここで、ユーザクライアント901よりアクセス要求があると、情報公開部1003は、ステップSE3の判断結果を「Yes」とする。

【0144】

ステップSE4では、情報公開部1003は、公開情報データベース1004（図13（b）参照）に基づいて、図14に示した情報公開画面1200をユーザクライアント901の表示部（図示略）に表示させる処理を実行する。この情報公開画面1200は、ユーザ900にセキュリティ情報（「返答情報」、「分類」、「セキュリティ情報の内容」、「返答者」および「修正方法」）を公開するための画面である。

【0145】

ステップSE5では、情報公開部1003は、ユーザ900により、情報公開画面1200の中から所望のセキュリティ情報が選択されたか否かを判断し、この場合、判断結果が「No」であるものとする。ステップSE8では、情報公開部1003は、アクセス解除されたか否か、具体的には終了ボタン1201（図14参照）が押下されたか否かを判断し、この場合、判断結果を「No」として、ステップSE5以降の処理を繰り返す。

【0146】

ここで、ユーザ900により、図14に示した返答番号3が入力されることにより、返答番号「3」に対応するセキュリティ情報が選択されると、情報公開部1003は、ステップSE5の判断結果を「Yes」とする。ステップSE6では、情報公開部1003は、返答番号「3」をキーとして、図13に示した公開

情報データベース1004を検索し、セキュリティ情報ポインタ「PS3」およびパッチ情報ポインタ「PP3」を取得する。

【0147】

つぎに、情報公開部1003は、セキュリティ情報ポインタ「PS3」およびパッチ情報ポインタ「PP3」に基づいて、公開情報データベース1004からセキュリティ情報800およびパッチ情報1100を取得する。ステップSE7では、情報公開部1003は、上記セキュリティ情報800およびパッチ情報1100をネットワーク502を介してユーザクライアント901へ転送する。ここで、ユーザ900により終了ボタン1201が押下されると、情報公開部1003は、ステップSE8の判断結果を「Yes」とし、ステップSE1以降の処理を繰り返す。

【0148】

また、セキュリティ情報800およびパッチ情報1100がユーザクライアント901に受信されると、ユーザ900は、セキュリティ情報800の内容を認識し、パッチ情報1100のパッチプログラムを「ソフトウェアX」に適用する。これにより、「ソフトウェアX」が修正される。

【0149】

なお、実施の形態4では、ユーザ900が所望するクライアント情報の分類情報を予め情報公開部1003に登録しておき、ユーザクライアント901からアクセス要求があった場合、当該分類情報に対応するセキュリティ情報（パッチ情報）を公開情報データベース1004から抽出し、これをユーザ900に対して公開するようにしてもよい。さらに、実施の形態4では、返答情報801および支払情報802に加えて、パッチ情報1100もユーザクライアント501に転送するようにしてもよい。

【0150】

以上説明したように、実施の形態4によれば、情報公開部1003によりセキュリティ情報を公開するようにしたので、セキュリティ情報の提供に関する第三者（ユーザ900）の関心を引くことができ、多数のセキュリティ情報の提供を期待することができる。また、実施の形態4によれば、パッチ情報1100をユ

ーザクライアント901（ユーザクライアント501）へ転送するようにしたので、迅速にセキュリティ情報に対する対策を講じることができる。

【0151】

以上本発明にかかる実施の形態1～4について図面を参照して詳述してきたが、具体的な構成例はこれら実施の形態1～4に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。

【0152】

例えば、前述した実施の形態1～4においては、セキュリティ情報を仲介する機能を実現するためのセキュリティ情報仲介プログラムを図17に示したコンピュータ読み取り可能な記録媒体1400に記録して、この記録媒体1400に記録されたセキュリティ情報仲介プログラムを同図に示したコンピュータ1300に読み込ませ、実行することによりセキュリティ情報の仲介を行うようにしてもよい。

【0153】

図17に示したコンピュータ1300は、上記セキュリティ情報仲介プログラムを実行するCPU1301と、キーボード、マウス等の入力装置1302と、各種データを記憶するROM（Read Only Memory）1303と、演算パラメータ等を記憶するRAM（Random Access Memory）1304と、記録媒体1400からセキュリティ情報仲介プログラムを読み取る読取装置1305と、ディスプレイ、プリンタ等の出力装置1306と、装置各部を接続するバスBUとから構成されている。

【0154】

CPU1301は、読取装置1305を経由して記録媒体1400に記録されているセキュリティ情報仲介プログラムを読み込んだ後、セキュリティ情報仲介プログラムを実行することにより、前述したセキュリティ情報の仲介を行う。なお、記録媒体1400には、光ディスク、フロッピーディスク、ハードディスク等の可搬型の記録媒体が含まれることはもとより、ネットワークのようにデータを一時的に記録保持するような伝送媒体も含まれる。

【0155】

【発明の効果】

以上説明したように、本発明によれば、情報提供者からのセキュリティ情報をダイレクトに情報受信者側に提供し、しかも有用なセキュリティ情報を提供した者に対して支払いを行うようにしたので、情報提供者（ユーザ）にとってセキュリティ情報を提供し易い環境を整備し、情報受信者（例えば、開発元）にとって低コストで有用なセキュリティ情報を収集することができるという効果を奏する。

【0156】

また、本発明によれば、情報提供者より提供されたセキュリティ情報が新規である場合にのみ、当該セキュリティ情報を情報受信者端末へ転送するようにしたので、不要なセキュリティ情報を情報受信者端末へ転送するという無駄を防止でき、効率良くセキュリティ情報の収集を行うことができるという効果を奏する。

【0157】

また、本発明によれば、情報受信者が所望するセキュリティ情報の分類情報を登録しておき、上記分類情報と、提供されたセキュリティ情報の分類結果とが一致する場合にのみ当該セキュリティ情報を情報受信者端末へ転送するようにしたので、不要なセキュリティ情報を情報受信者端末へ転送するという無駄を防止でき、さらに効率良くセキュリティ情報の収集を行うことができるという効果を奏する。

【0158】

また、本発明によれば、情報提供者から提供されたセキュリティ情報の無効を示す無効情報を情報提供者端末へ転送するようにしたので、提供したセキュリティ情報の使われ方（有用または無効）に関心を持つ情報提供者に対するサービスを向上させることができるという効果を奏する。

【0159】

また、本発明によれば、有用性が示されたセキュリティ情報の対策用の修正情報を情報提供者端末へ転送するようにしたので、迅速にセキュリティ情報に対する対策を講じることができるという効果を奏する。

【0160】

また、本発明によれば、セキュリティ情報を公開するようにしたので、セキュリティ情報の提供に関する第三者の関心を引くことができ、多数のセキュリティ情報の提供を期待することができるという効果を奏する。

【0161】

また、本発明によれば、セキュリティ情報および修正情報を公開するようにしたので、セキュリティ情報の提供に関する第三者の関心を引くことができ、多数のセキュリティ情報の提供を期待することができるとともに、迅速にセキュリティ情報に対する対策を講じることができるという効果を奏する。

【図面の簡単な説明】

【図1】

本発明にかかる実施の形態1の構成を示すブロック図である。

【図2】

図1に示したセキュリティ情報40、返答情報41A、41Bおよび支払情報42を示す図である。

【図3】

同実施の形態1の動作を説明するフローチャートである。

【図4】

本発明にかかる実施の形態2の構成を示すブロック図である。

【図5】

図4に示したセキュリティ情報400A、400B、返答情報401A、401Bおよび支払情報402を示す図である。

【図6】

図4に示したセキュリティ情報データベース203および返答情報データベース204のデータ構造を示す図である。

【図7】

同実施の形態2の動作を説明するフローチャートである。

【図8】

本発明にかかる実施の形態3の構成を示すブロック図である。

【図9】

図 8 に示したセキュリティ情報 800、返答情報 801、支払情報 802 および分類情報 803A、803B を示す図である。

【図 10】

図 8 に示したセキュリティ情報データベース 603、返答情報データベース 604 および分類情報データベース 606 のデータ構造を示す図である。

【図 11】

同実施の形態 3 の動作を説明するフローチャートである。

【図 12】

本発明にかかる実施の形態 4 の構成を示すブロック図である。

【図 13】

図 12 に示した返答情報データベース 1002、公開情報データベース 1004 およびパッチ情報 1100 のデータ構造を示す図である。

【図 14】

同実施の形態 4 における情報公開画面 1200 の一例を示す図である。

【図 15】

同実施の形態 4 の動作を説明するフローチャートである。

【図 16】

図 12 に示した情報公開部 1003 の動作を説明するフローチャートである。

【図 17】

本発明にかかる実施の形態 1～4 の変形例を示すブロック図である。

【符号の説明】

- 11 ユーザクライアント
- 20 セキュリティ情報仲介装置
- 21 セキュリティ情報登録部
- 23 転送部
- 26 転送部
- 101A ユーザクライアント
- 200 セキュリティ情報仲介装置
- 201 受信部

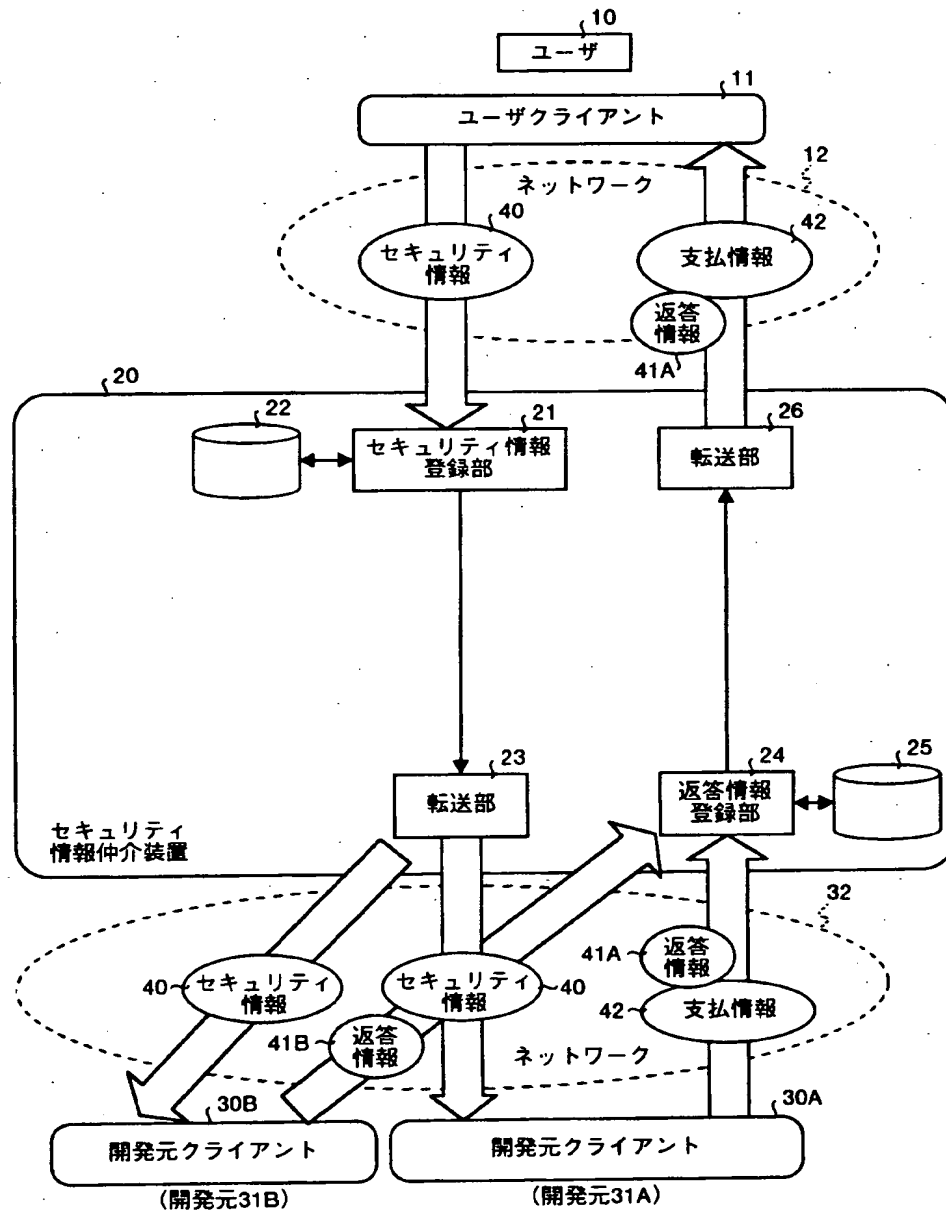
2 0 2 情報管理部
2 0 5 転送部
2 0 6 受信部
2 0 7 転送部
3 0 0 開発元クライアント
5 0 1 ユーザクライアント
6 0 0 セキュリティ情報仲介装置
6 0 1 受信部
6 0 2 情報管理部
6 0 5 転送部
6 0 7 受信部
6 0 8 転送部
7 0 0 A 開発元クライアント
9 0 1 ユーザクライアント
1 0 0 0 セキュリティ情報仲介装置
1 0 0 1 情報管理部
1 0 0 3 情報公開部
1 3 0 0 コンピュータ
1 3 0 1 CPU
1 4 0 0 記録媒体

【書類名】

図面

【図 1】

実施の形態 1 の構成を示すブロック図



【図 2】

図 1 に示したセキュリティ情報40、返答情報41A、41B および
支払情報42を示す図

40；セキュリティ情報

(a)

登録者	セキュリティ情報の内容
ユーザ10	ソフトウェアXのバグ問題

41A；返答情報

(b)

返答者	判定結果	登録者	セキュリティ情報の内容
開発元31A	有効	ユーザ10	ソフトウェアXのバグ問題

41B；返答情報

(c)

返答者	判定結果	登録者	セキュリティ情報の内容
開発元31B	無効	ユーザ10	ソフトウェアXのバグ問題

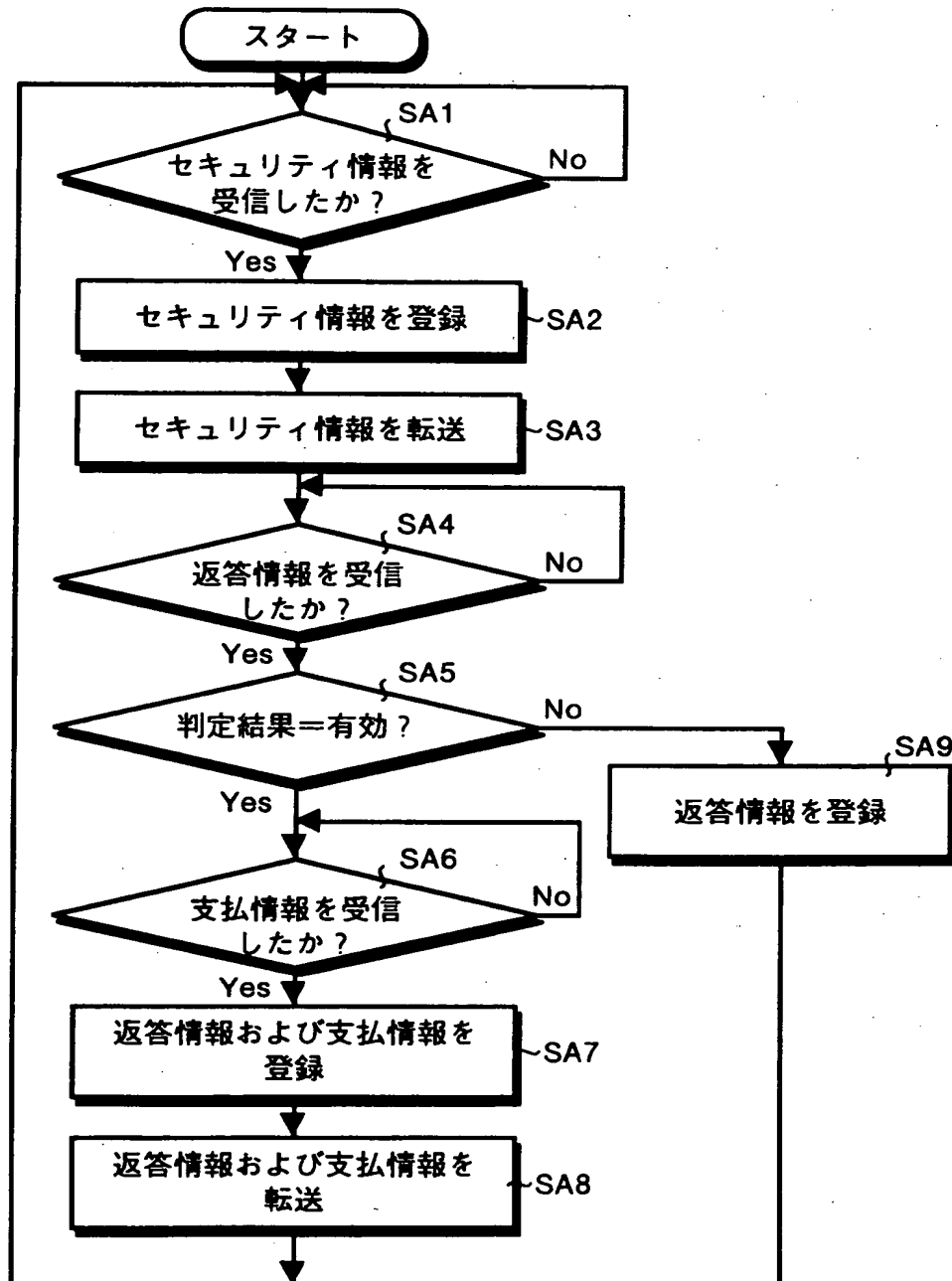
42；支払情報

(d)

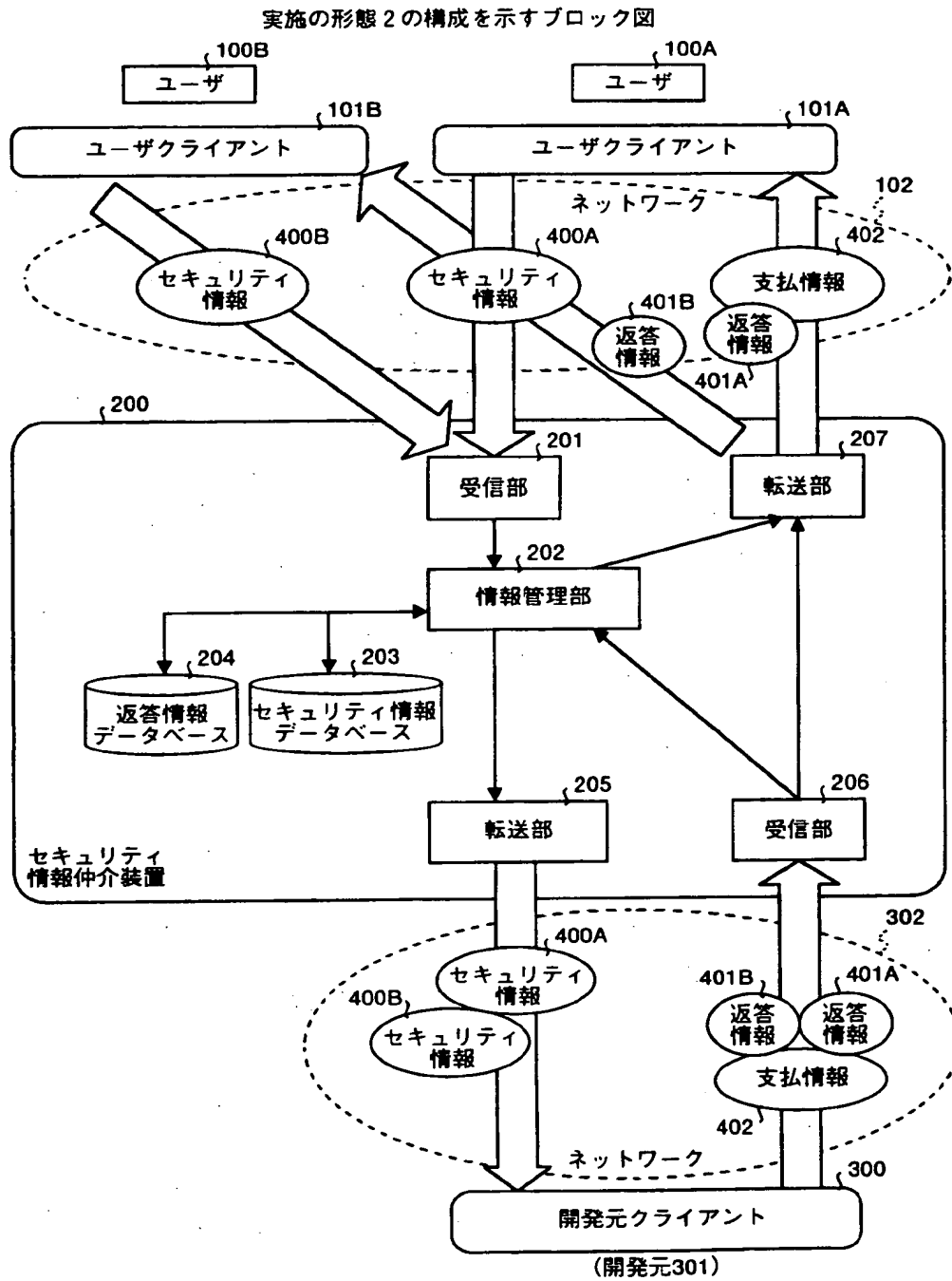
支払金額	支払先	支払者	支払方法
10000円	ユーザ10	開発元31A	電子決済

【図 3】

実施の形態 1 の動作を説明するフローチャート



【図 4】



【図 5】

図 4 に示したセキュリティ情報400A、400B、返答情報401A、401B
および支払情報402を示す図

400A；セキュリティ情報

(a)

登録者	セキュリティ情報の内容
ユーザ100A	ソフトウェアXのバグ問題QA

400B；セキュリティ情報

(b)

登録者	セキュリティ情報の内容
ユーザ100B	ソフトウェアXのバグ問題QB

401A；返答情報

(c)

返答者	判定結果	登録者	セキュリティ情報の内容
開発元301	有効	ユーザ100A	ソフトウェアXのバグ問題QA

401B；返答情報

(d)

返答者	判定結果	登録者	セキュリティ情報の内容
開発元301	無効	ユーザ100B	ソフトウェアXのバグ問題QB

402；支払情報

(e)

支払金額	支払先	支払者	支払方法
10000円	ユーザ100A	開発元301	電子決済

【図 6】

図 4 に示したセキュリティ情報データベース203
および返答情報データベース204のデータ構造を示す図

(a)

203；セキュリティ情報データベース

登録番号	登録日時	登録者	セキュリティ情報の内容
1	2000/4/27 18:00:13	ユーザy	ソフトウェアYのバグ問題
2	2000/5/13 14:32:10	ユーザz	ソフトウェアZのバグ問題
3	2000/6/11 19:26:30	ユーザ100A	ソフトウェアXのバグ問題QA
4	2000/7/25 08:10:40	ユーザ100B	ソフトウェアXのバグ問題QB

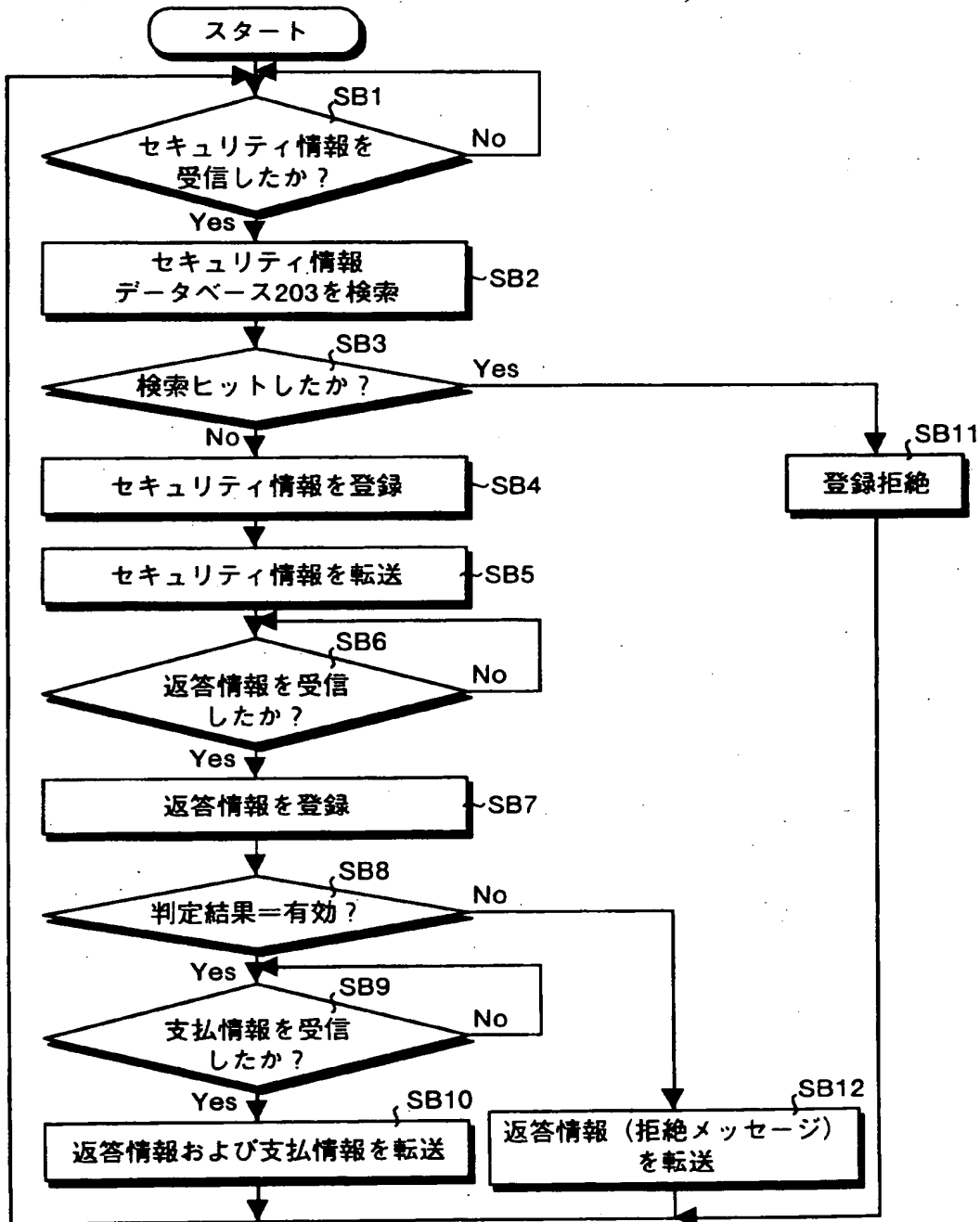
(b)

204；返答情報データベース

返答番号	返答日時	登録番号	返答者	判定結果
1	2000/4/28 12:26:14	1	開発元301	有効
2	2000/5/14 15:33:20	2	開発元301	無効
3	2000/6/12 19:36:40	3	開発元301	有効
4	2000/7/26 10:15:55	4	開発元301	無効

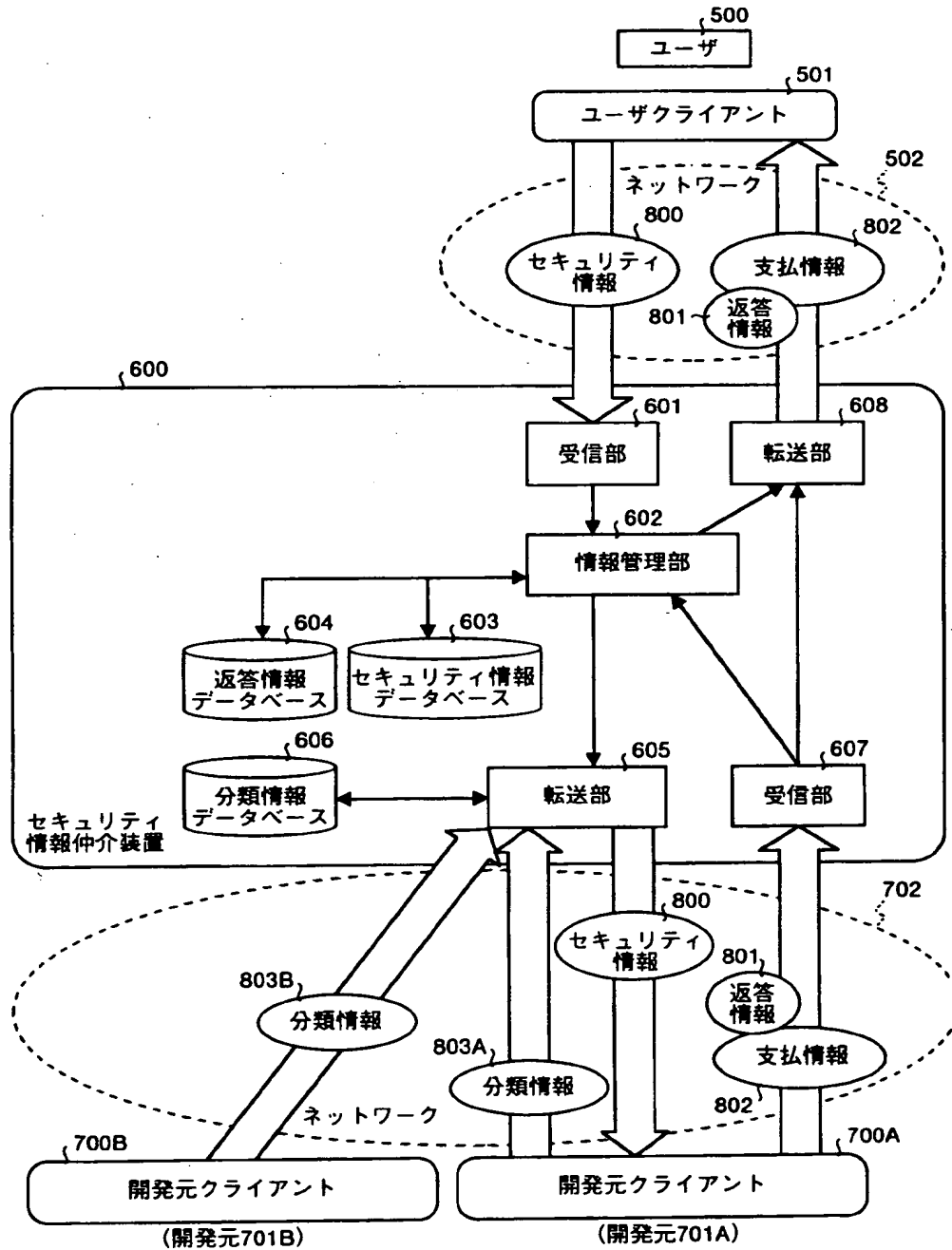
【図 7】

実施の形態 2 の動作を説明するフローチャート



【図 8】

実施の形態 3 の構成を示すブロック図



【図 9】

図 8 に示したセキュリティ情報800, 返答情報801, 支払情報802
および分類情報803A, 803Bを示す図

- (a) 800; セキュリティ情報
- | 登録者 | セキュリティ情報の内容 |
|--------|--------------|
| ユーザ500 | ソフトウェアXのバグ問題 |
- (b) 801; 返答情報
- | 返答者 | 判定結果 | 登録者 | 分類 | セキュリティ情報の内容 |
|---------|------|--------|----|--------------|
| 開発元701A | 有効 | ユーザ500 | A | ソフトウェアXのバグ問題 |
- (c) 802; 支払情報
- | 支払金額 | 支払先 | 支払者 | 支払方法 |
|--------|--------|---------|------|
| 10000円 | ユーザ500 | 開発元701A | 電子決済 |
- (d) 803A; 分類情報
- | 開発元 | 分類 |
|---------|----|
| 開発元701A | A |
- (e) 803B; 分類情報
- | 開発元 | 分類 |
|---------|----|
| 開発元701B | B |

【図 10】

図 8 に示したセキュリティ情報データベース603、返答情報データベース604
および分類情報データベース606のデータ構造を示す図

(a)

603；セキュリティ情報データベース

登録番号	登録日時	登録者	分類	セキュリティ情報の内容
1	2000/4/27 18:00:13	ユーザy	B	ソフトウェアYのバグ問題
2	2000/5/13 14:32:10	ユーザz	B	ソフトウェアZのバグ問題
3	2000/6/11 19:26:30	ユーザ500	A	ソフトウェアXのバグ問題

(b)

604；返答情報データベース

返答番号	返答日時	登録番号	返答者	分類	判定結果
1	2000/4/28 12:26:14	1	開発元701B	B	有効
2	2000/5/14 15:33:20	2	開発元701B	B	無効
3	2000/6/12 19:36:40	3	開発元701A	A	有効

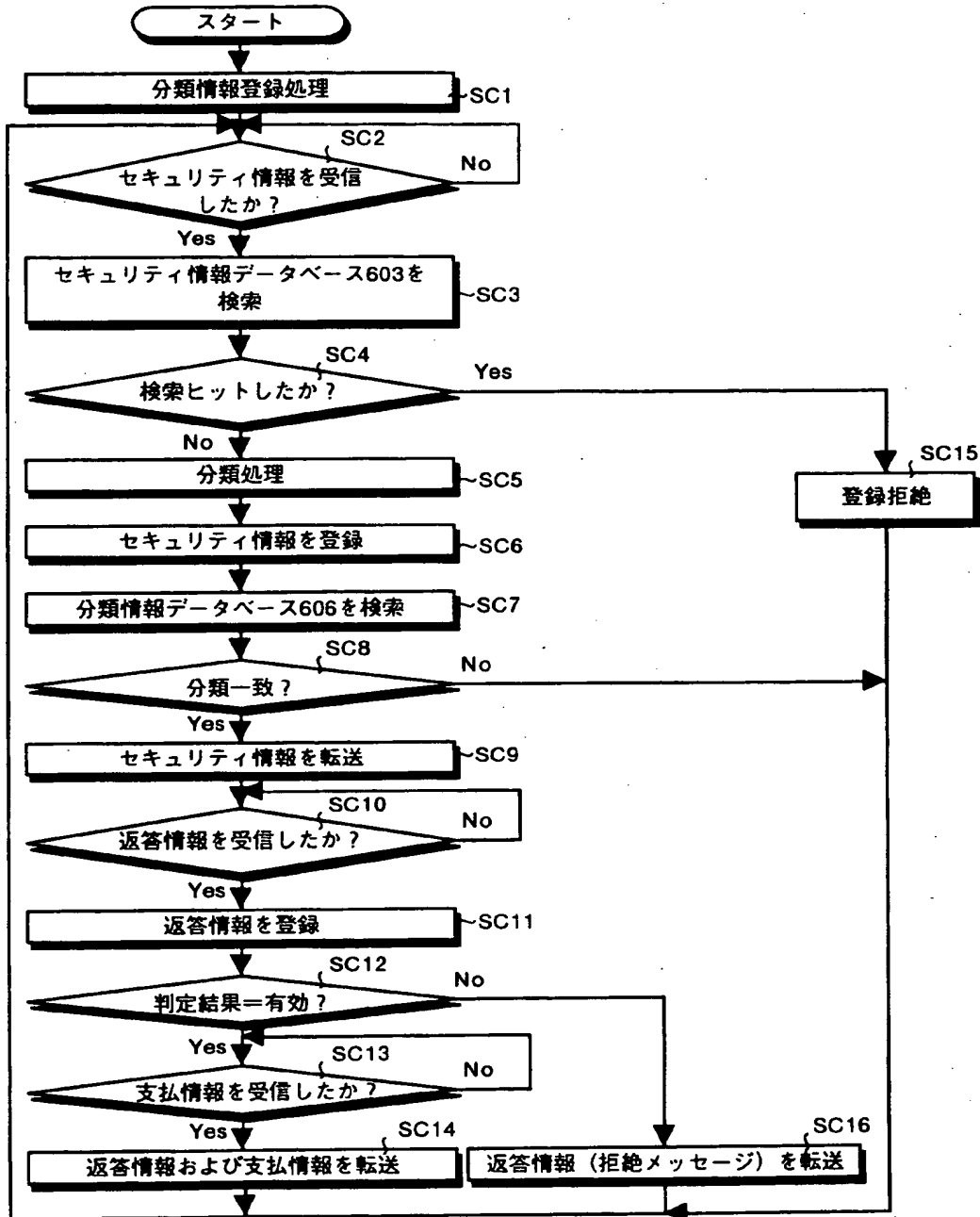
(c)

606；分類情報データベース

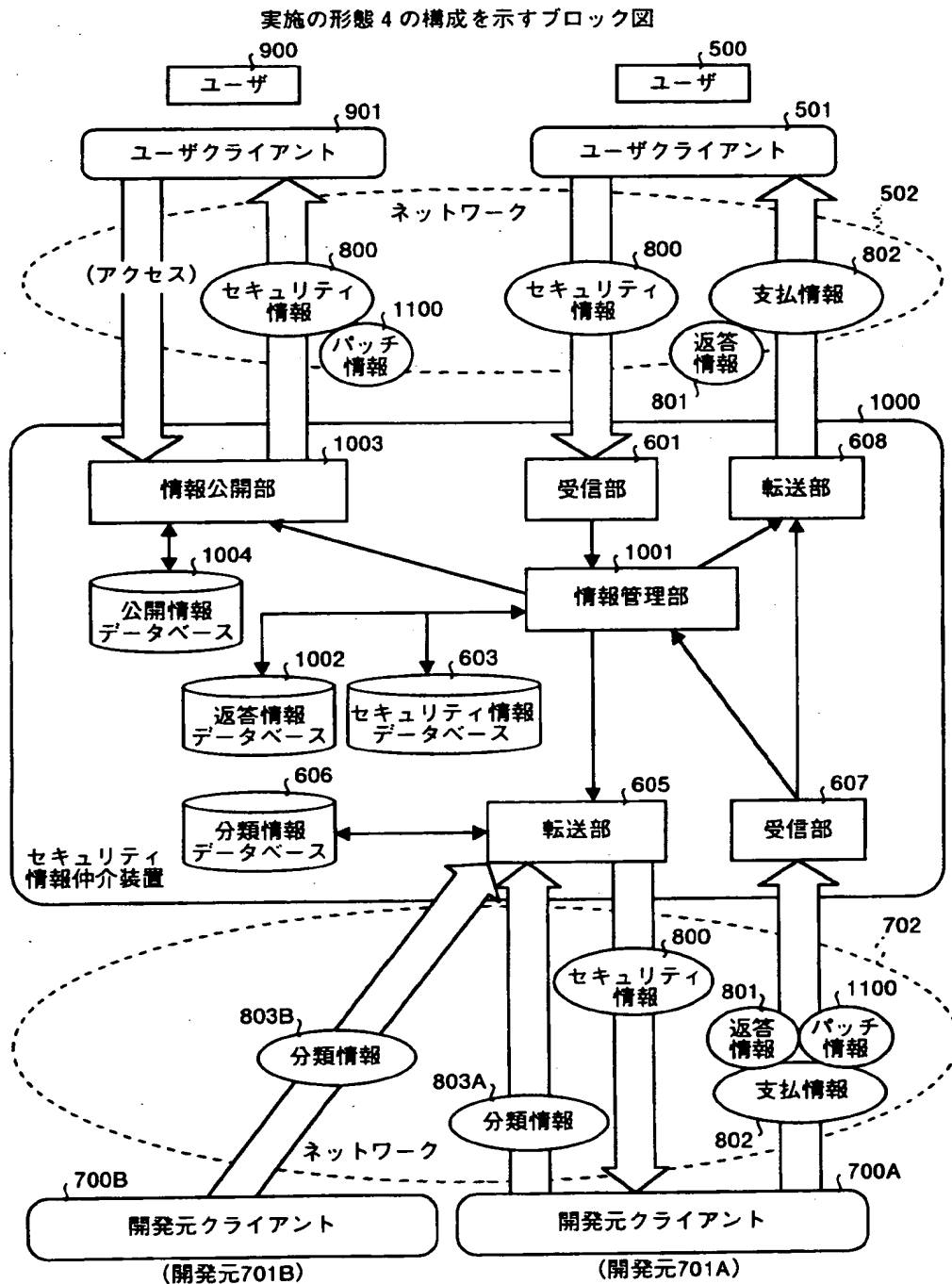
開発元	分類
開発元701A	A
開発元701B	B

【図 11】

実施の形態 3 の動作を説明するフローチャート



【図 12】



【図 1 3】

図12に示した返答情報データベース1002、公開情報データベース1004
およびパッチ情報1100のデータ構造を示す図

(a)

1002；返答情報データベース

返答番号	返答日時	登録番号	返答者	分類	判定結果	修正方法
1	2000/4/28 12:26:14	1	開発元701B	B	有効	パッチ
2	2000/5/14 15:33:20	2	開発元701B	B	無効	
3	2000/6/12 19:36:40	3	開発元701A	A	有効	パッチ

(b)

1004；公開情報データベース

返答番号	分類	セキュリティ情報の内容	返答者	修正方法	セキュリティ情報ホインタ	パッチ情報ホインタ
3	A	ソフトウェアの ハック問題	開発元 701A	パッチ	PS3	PP3

(c)

1100；パッチ情報

返答番号	返答者	
3	開発元701A	パッチプログラム

【図 1 4】

実施の形態 4 における情報公開画面1200の一例を示す図

1200；情報公開画面

現在、つぎのセキュリティ情報を公開しております。

返答番号	分類	セキュリティ情報の内容	返答者	修正方法
3	A	ソフトウェアXの バグ問題	開発元 701A	パッチ

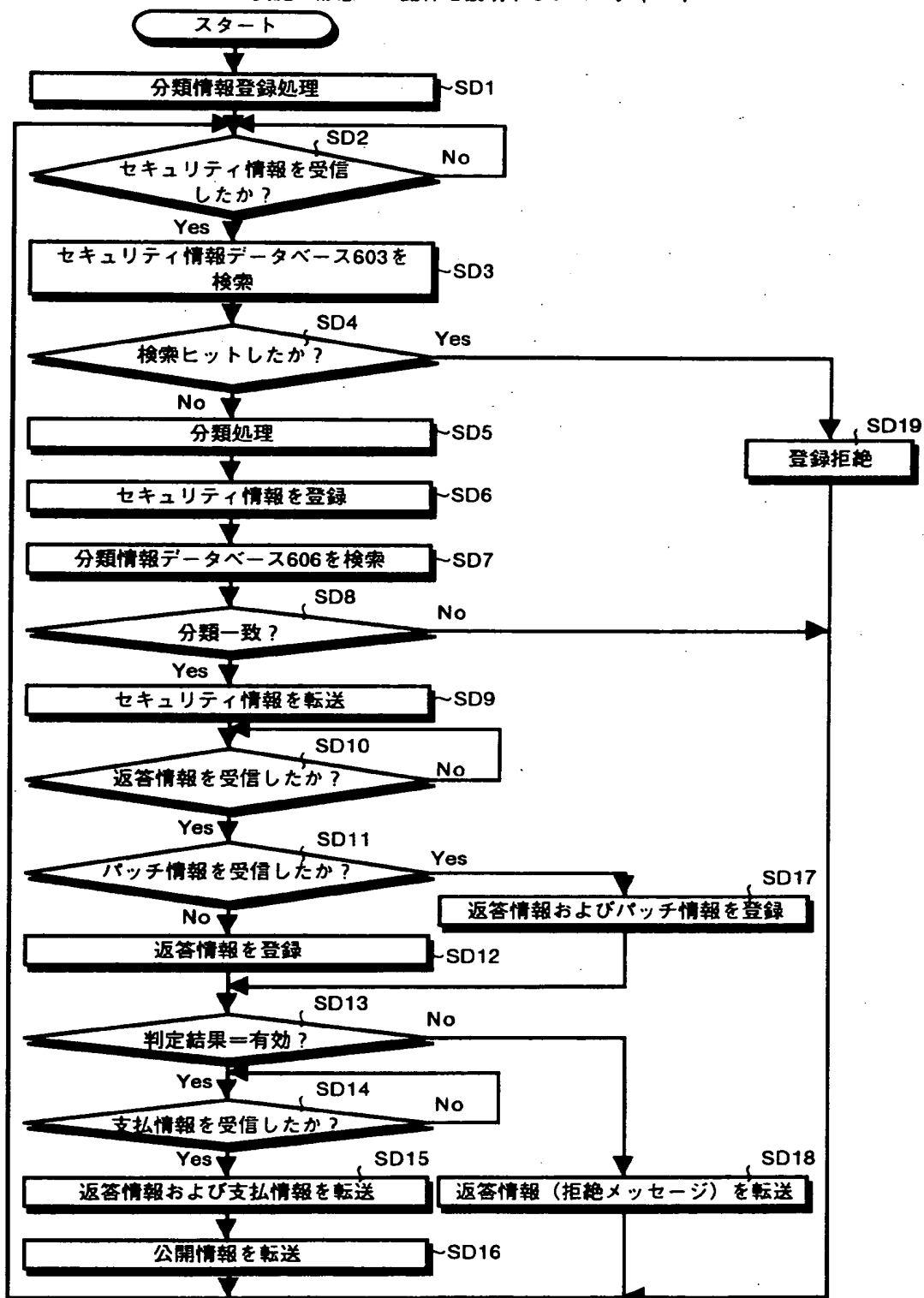
返答番号によりセキュリティ情報を選択して下さい。
送信を開始します。
返答番号：3

1201

終了

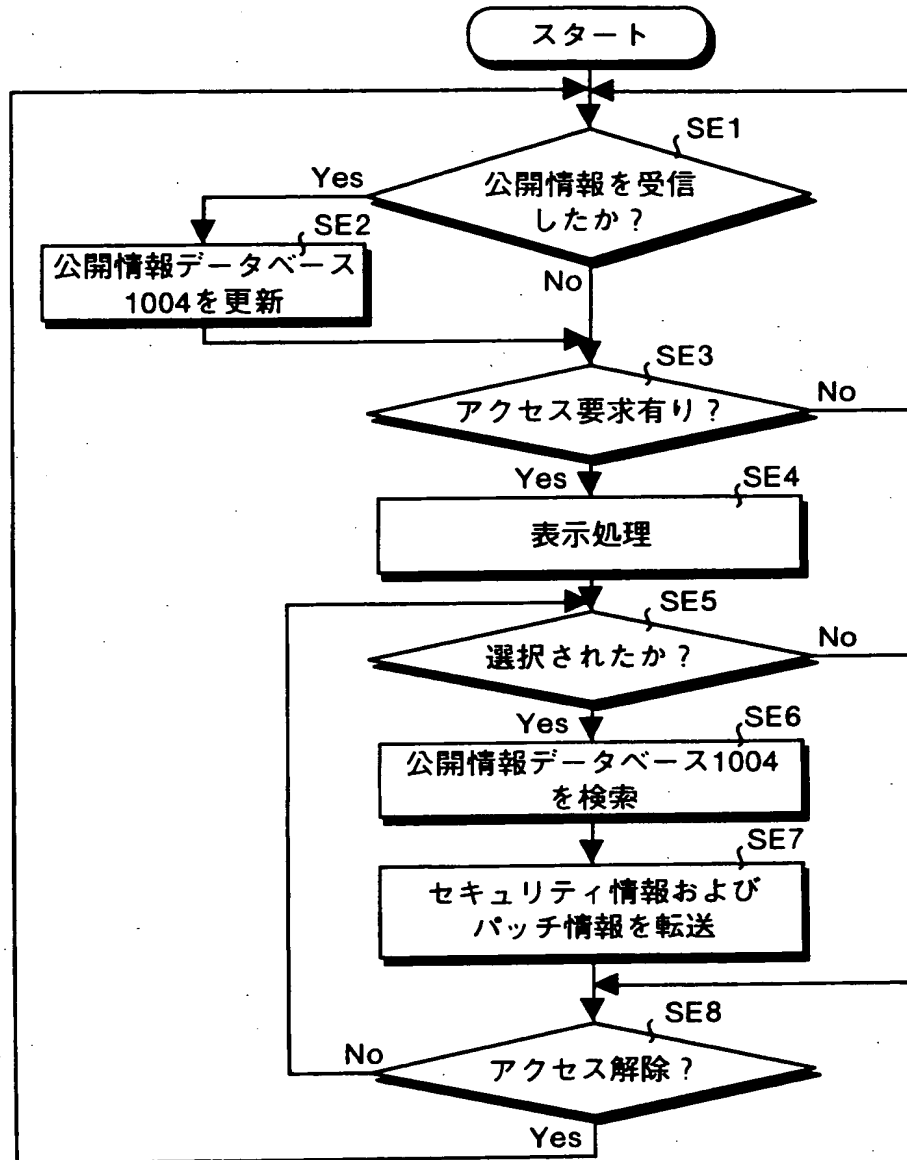
【図 15】

実施の形態 4 の動作を説明するフローチャート



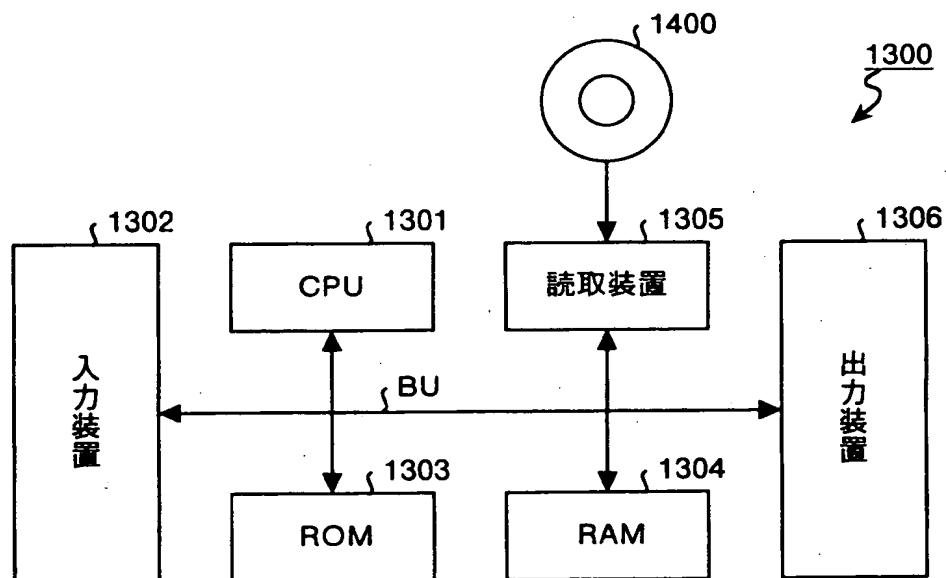
【図16】

図12に示した情報公開部1003の動作を説明するフローチャート



【図 1 7】

実施の形態 1 ～ 4 の変形例を示すブロック図



【書類名】 要約書

【要約】

【課題】 ユーザにとってセキュリティ情報を提供し易い環境を整備し、開発元にとって低コストで有用なセキュリティ情報を収集すること。

【解決手段】 ユーザクライアント 1 1 から提供されたセキュリティ情報 4 0 を登録するセキュリティ情報登録部 2 1 と、セキュリティ情報 4 0 の有用性を判断する開発元 3 1 A の開発元クライアント 3 0 A へ、セキュリティ情報登録部 2 1 により登録されたセキュリティ情報 4 0 を転送する転送部 2 3 と、セキュリティ情報 4 0 の有用性を示す返答情報 4 1 A および当該セキュリティ情報 4 0 の情報提供料の支払いに関する支払情報 4 2 を開発元クライアント 3 0 A より受信する返答情報登録部 2 4 と、返答情報 4 1 A および支払情報 4 2 をユーザクライアント 1 1 へ転送する転送部 2 6 とを備えている。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社